

Franks Edison González Landero

Diseño de un sistema ciberfísico aplicado al ámbito de la salud.

Director/es

Dr. D. García-Magariño García, Iván
Dra. D^a. Lacuesta Gilaberte, Raquel

<http://zaguan.unizar.es/collection/Tesis>



Universidad
Zaragoza

Tesis Doctoral

**DISEÑO DE UN SISTEMA CIBERFÍSICO APLICADO
AL ÁMBITO DE LA SALUD.**

Autor

Franks Edison González Landero

Director/es

Dr. D. García-Magariño García, Iván
Dra. D^a. Lacuesta Gilaberte, Raquel

UNIVERSIDAD DE ZARAGOZA
Escuela de Doctorado

2021

Diseño de un sistema ciberfísico aplicado
al ámbito de la salud.



Universidad
Zaragoza

TESIS DOCTORAL
Bajo la dirección de los doctores
Ivan García-Magariño García
Raquel Lacuesta Gilaberte

Franks Edison González Landero
Departamento de Informática e Ingeniería de sistemas
Escuela Universitaria Politécnica de Teruel
Universidad de Zaragoza

Junio 2021

Documento maquetado con T_EX_S v.1.0+.

Diseño de un sistema ciberfísico aplicado al ámbito de la salud.

Memoria que presenta para optar al título de Doctor en Informática

Franks Edison González Landero

Dirigida por los Doctores

Iván García-Magariño García y Raquel Lacuesta Gilaberte

Departamento de Informática e Ingeniería de sistemas

Escuela Universitaria Politécnica de Teruel

Universidad de Zaragoza

Junio 2021

A mis padres

*Admitámoslo, esto no es
lo peor que me has visto hacer.
Anthony Edward Stark*

Acerca de este documento

Esta Tesis Doctoral se presenta como compendio de publicaciones editadas, de acuerdo al extracto de 25/06/2020 del Consejo de Gobierno de la Universidad de Zaragoza por el que se aprueba el Reglamento Sobre Tesis Doctorales (Título IV, Capítulo III, artículo 20).

Los artículos que se aportan como primera autoría y forman parte de la Tesis Doctoral son los siguientes:

- GONZÁLEZ-LANDERO, F., GARCÍA-MAGARIÑO, I., AMARIGLIO, R., & LACUESTA, R. (2019). Smart cupboard for assessing memory in home environment. *Sensors*, 19(11), 2552.

- GONZÁLEZ-LANDERO, F., GARCÍA-MAGARIÑO, I., LACUESTA, R., & LLORET, J. (2018). PriorityNet App: A mobile application for establishing priorities in the context of 5G ultra-dense networks. *IEEE Access*, 614141-14150.

- GONZÁLEZ-LANDERO, F., GARCÍA-MAGARIÑO, I., LACUESTA, R., & LLORET, J. (2018). Green communication for tracking heart rate with smartbands *Sensors*, 18(8), 2652.

- GONZÁLEZ-LANDERO, F., GARCÍA-MAGARIÑO, I., LACUESTA, R., & LLORET, J. (2018). ABS-DDoS: An Agent-Based Simulator about Strategies of Both DDoS Attacks and Their Defenses, to Achieve Efficient Data Forwarding in Sensor Networks and IoT Devices *Wireless Communications and Mobile Computing*, 2018.

El artículo que se aporta como coautor y forma parte de la tesis doctoral es el siguiente:

- GARCÍA-MAGARIÑO, I., GONZÁLEZ-LANDERO, F., AMARIGLIO, R., & LLORET, J. (2019). Collaboration of smart IoT devices exem-

plified with smart cupboards. *IEEE Access*, 7, 9881-9892.

Este documento, de acuerdo a la normativa actual, expone los siguientes requisitos:

- Una página inicial en la que se especifica que la tesis es un compendio de trabajos previamente publicados o aceptados para su publicación. En ella se hace constar las referencias completas de los artículos que constituyen el cuerpo de la tesis.
- Una introducción general en la que se presentan los objetivos de la tesis y los trabajos realizados y se justifique la unidad temática de los mismos, acompañada de una revisión bibliográfica de los conocimientos previos en los que se basan los trabajos publicados.
- Una copia de los trabajos publicados o aceptados para su publicación.
- Una discusión global de los trabajos aportados y las conclusiones finales de la tesis.
- Un apéndice en el que se incluirán las copias de las cartas de aceptación de los trabajos pendientes de publicación, el factor de impacto de las revistas y áreas temáticas correspondientes a las publicaciones que se recogen en la tesis y la justificación de la contribución del doctorando si se trata de un trabajo realizado en coautoría.

Agradecimientos

La realización de esta tesis es el fruto de muchos esfuerzos y sacrificios que suponen el último y más importante grado académico que me ofrece la vida universitaria. Como ya he manifestado a muchos de mis allegados no he realizado este camino con el fin de obtener prestigio como investigador o perseguir un determinado puesto, ya que mi principal campo de trabajo es el empresarial. Mi principal fin siempre ha sido el ampliar conocimientos y aprender más del área tecnológica, sin embargo en esta ocasión preferí salirme de mi zona de confort. Bajo esta premisa me acerque a uno de mis directores, Iván, el cual aceptó ser mi director y al cual le debo todo lo que he aprendido en este periodo tiempo. A él le agradezco todos sus consejos para convertirme en un buen investigador, también le agradezco todo su trabajo, absoluta devoción conmigo, ser fuente de inspiración en momentos difíciles y por los buenos momentos que pasamos en paralelo a esta investigación. Aparentemente, no hay problema que él no pueda resolver.

Le agradezco mucho a mi otra directora, Raquel, por ser ese punto crítico y la persona que aportó la “guinda” a cada artículo publicado. También le agradezco por su infinita paciencia y dedicación a la redacción de esta tesis, su implicación es muy meritoria en estos tiempos de inmediatez. Nadie me diría que durante la realización de esta tesis tropezaría con momentos alegres y divertidos, como la difusión radial y televisada en la que fui participe con ella, nuevamente gracias por estar ahí conmigo.

Quiero agradecerle también a Elena, por brindarme todo su cariño y apoyo durante gran parte de este recorrido. Me quedo sin palabras para reconocerle toda la paciencia y sacrificios diarios que hace por ambos mientras yo construía este documento

Por supuesto no puedo olvidarme de mis padres por su infinito amor y apoyo incondicional. Me inculcaron la cultura del esfuerzo y a pesar de que en un primer momento no confiaba en mí, gracias a ellos estoy escribiendo estas líneas.

No puedo olvidarme de todas aquellas personas que hicieron parte de mis experimentos de manera voluntaria. Creo que esta ha sido una de las partes más duras de cada artículo realizado dado que muchas personas tienen su rutina y se ven obligadas a romperla por que yo se los pido. Dado que la

cantidad de gente ha sido enorme, si has sido uno de los voluntarios y estas leyendo estas líneas quiero que sepas que te estoy muy agradecido.

Finalmente, no puedo olvidarme de mi perro Joker. Puedo afirmar sin mentir que ha estado completamente a mi lado desde que vivimos juntos. Se ha mantenido a mi lado cada tarde de escritura, y si él pudiera hablar podría atestiguar cada quebradero de cabeza que me ha surgido y la manera cómo lo he solucionado. Además, con sus tiernos gestos me indicaba que ya era momento de parar, despejarme y dar una vuelta, acción que en muchos momentos me vino bien para seguir con más fuerza y decisión.

Finalmente, mi agradecimiento a Dios, toda la gloria sea para él.

Resumen

Los Sistemas Ciber-Físicos (CPS) tienen la capacidad de coordinar el tratamiento de datos y sistemas de comunicación con el seguimiento y control de las entidades que se encuentran en el entorno físico. Estos sistemas están formados por un conjunto de dispositivos como: sensores, unidades de procesamiento, dispositivos de comunicación y en muchos casos servicios en la nube. Debido a la naturaleza de los distintos tipos de hardware un CPS puede estar formado por múltiples dispositivos con diferentes arquitecturas, protocolos e interfaces y en una gran parte de los casos los CPS son sistemas híbridos y distribuidos.

Esta tesis presenta el diseño de un CPS enfocado al entorno de la salud. En el diseño del CPS se han tenido en cuenta tanto aspectos de implementación a nivel físico, como análisis de medidas de seguridad, el diseño de la interacción y un modelo energético acorde. A nivel físico se ha decidido implementar un armario inteligente de cocina el cual posee internamente una placa de procesamiento que se encarga de recopilar las aperturas y los cierres que se efectúen en este. La función principal del armario es realizar un seguimiento de los usuarios para la detección de síntomas asociados a enfermedades neurodegenerativas como el Alzheimer. En relación a la seguridad expone una herramienta que permita tomar las medidas de seguridad más adecuadas para evitar ataques de denegación de servicios (DoS) de tal manera que el normal funcionamiento del sistema no se vea comprometido. Otro elemento que tiene en cuenta es la manera de interactuar con el usuario, el cual es objeto de estudio según el tipo de usuario que esté usando el CPS. Finalmente se propone un modelo de consumo energético, el cual se basa en la rutina del usuario para efectuar un consumo de energía en los momentos más álgidos del día en relación al estilo de vida del usuario.

Índice

Acerca de este documento	IX
Agradecimientos	XI
Resumen	XIII
1. Introducción	1
1.1. Contexto de los sistemas ciberfísicos aplicados a la salud.	3
1.2. Contribución de los sistemas ciber físicos aplicados a la salud.	7
1.3. Conclusiones de la introducción	8
2. Estado del arte	11
2.1. Sistemas ciber-físicos aplicados al cuidado de la salud.	14
2.2. Muebles inteligentes aplicados al cuidado de la salud.	16
2.3. Internet of things aplicado al Alzheimer.	17
2.4. Seguridad en sistemas ciber-físicos.	18
2.5. Dispositivos inteligentes	20
2.6. Eficiencia energética	23
3. Objetivos y planteamiento de la tesis	27
3.1. Objetivos generales.	28
3.1.1. La elección del componente físico en el CPS.	30
3.1.2. Interacción del usuario con el CPS.	31
3.1.3. Herramientas de medición.	32
3.1.4. Sistema de alimentación del CPS.	33
3.1.5. Medidas de seguridad.	34
3.2. Discusión	37
3.3. Planteamiento del trabajo: Armario inteligente.	45
4. Discusión integradora de artículos resentados	55
4.1. Componente físico del CPS.	55
4.2. Interacción con los perfiles de usuarios.	58

4.2.1. Configuración del CPS	58
4.2.2. Interacción natural con el usuario	61
4.3. Monitorización técnica del CPS al usuario.	62
4.4. Modelo de alimentación eléctrica.	65
4.5. Seguridad en el CPS: Simulador ABS-DDoS.	67
5. Conclusiones y trabajo futuro	71
5.1. Trabajo futuro	75
6. Artículos presentados	79
6.1. Collaboration of smart IoT devices exemplified with smart cupboards.	80
6.2. Smart cupboard for assessing memory in home environment. .	92
6.3. PriorityNet App: A mobile application for establishing priori- ties in the context of 5G ultra-dense networks.	114
6.4. Green communication for tracking heart rate with smartbands.	125
6.5. ABS-DDoS: An agent-based simulator about strategies of both DDoS attacks and their defenses, to achieve efficient data for- warding in sensor networks and IoT devices.	147
I Apéndices	159
A. Factor de impacto de las publicaciones	161
A.1. Trabajos en primera autoría	161
A.2. Trabajos en coautoría	162
Bibliografía	163

Índice de figuras

2.1. Mapa conceptual sobre los CPS. Parte I	12
2.2. Mapa conceptual sobre los CPS. Parte II	13
3.1. Placas de procesamiento	43
4.1. Primer prototipo del Armario	56
4.2. Foto del armario final	57
4.3. Ejemplo del contenido de cada elemento de la aplicación en formato JSON	61
4.4. Sensores de puerta	62
4.5. Mecanismo técnico del CPS para detectar olvidos	63

Índice de Tablas

3.1. Clasificación taxonómica de los ataques a los RFID	35
3.2. Categorización y clasificación taxonómica de los ataques DoS en WSNs	36
3.3. Criterios de selección del componente físico	38
4.1. Precio de los componentes hardware del CPS	58

Capítulo 1

Introducción

El término CPS se refiere a todo aquel dispositivo que integra capacidades de computación, almacenamiento y comunicación para controlar e interactuar con un proceso físico. Estos dispositivos están, normalmente, conectados entre sí y también con servicios remotos de almacenamiento y gestión de datos. Hasta hace unos años era muy habitual que en los procesos de fabricación las máquinas estuviesen aisladas entre sí, estas generaban datos e información pero no existía una interacción entre máquinas o procesos. Actualmente existen más dispositivos conectados a diferentes tipos de redes que son capaces de captar información, y en base a esa información son capaces de interactuar con otras máquinas o dispositivos. Por ejemplo, un sensor de temperatura puede dedicarse solamente a registrar la temperatura de funcionamiento de una máquina, pero gracias a los sistemas de comunicación y al software puede llevar a cabo una automatización de tareas como sería parar esa máquina en caso de que supere un umbral de temperatura.

Un CPS normalmente está formado por sensores con conectividad, por dispositivos del Internet de las Cosas (IoT) que son capaces de generar datos y enviarlos o por robots que pueden realizar diferentes tareas. Estos dispositivos que guardan estrecha relación con los CPS generan información, la envían a los servidores en tiempo real y en ese momento se ponen en marcha herramientas de analítica de datos, que pueden tener o no, inteligencia artificial y que son capaces de dar órdenes a otras máquinas o dispositivos. Este proceso de captar información, transmitirla y disponer de automatismos se aplica en redes eléctricas inteligentes (Green et al., 2013), en sistemas de autonomía vehicular (Chen et al., 2017), en sistemas de monitorización en medicina y salud (Merlo et al., 2019), control de procesos (Zhang et al., 2017), robótica (Park et al., 2020) y domótica en nuestros hogares (Morón et al., 2016), aportando una gran relevancia a muchos ecosistemas industriales y científicos.

Toda esta comunicación entre componentes puede dar lugar a confusión entre conceptos. Esto es factible ya que hay otros términos que tienen matices parecidos y que van de la mano con el concepto de CPS, estos conceptos son comunicación máquina a máquina (M2M) e IoT.

Por un lado, el concepto de M2M es propuesto por la industria de las comunicaciones. La comunicación M2M se refiere a la comunicación de dispositivos mecánicos que no tienen la capacidad de comunicarse con otros de forma inherente, de manera que usan redes de comunicación móvil para ello. Con el paso del tiempo, este concepto se ha ido ampliando hasta abarcar la interacción y el intercambio de información con personas y equipos, dando sendos conceptos de comunicación humano a máquina (H2M) y máquina a humano (M2H). El concepto de M2M establece un marco técnico de comunicación que establece las bases de la conexión entre cosas y objetos. A través de tecnologías como la WiFi se logra una conexión confiable de extremo a extremo y permite operaciones como centralizado remoto, monitoreo de equipos, operaciones de logística y almacenamiento.

Por otro lado, en 1999, el Instituto de Tecnología de Massachusetts (MIT) propuso el concepto de IoT basado en la tecnología de los Identificadores de Radio Frecuencia (RFID). Tal concepto indicaba que todos los elementos conectados a Internet eran identificados por RFID para realizar actividades de gestión e identificación inteligente (Gubbi et al., 2013). Hoy en día, IoT es un concepto sobre el que se apoyan las empresas de Internet, las de software y la industria de toda información. Una vez que se ha conseguido la interconexión social entre las personas en sus distintas variantes, mensajes de texto, videos, redes sociales, las empresas esperan que las cosas también se puedan comunicar a través de Internet. El concepto de IoT principalmente enfatiza la participación de Internet en las transacciones que correspondan. La globalización, la apertura, la interoperabilidad y la socialización de Internet son la base para apoyar el concepto de IoT. Cuando un objeto o una “cosa” tiene una “identificación en la red”, puede generar una variedad de aplicaciones de Internet: productos inteligentes compartidos, servicios de información, pagos electrónicos y análisis de datos grandes entre otros. Si incluimos el concepto de M2M las posibilidades de servicios crecen exponencialmente, ya que es un término que por definición se lleva muy bien con el IoT.

Los CPS se especializan en procesos de retroalimentación y la circulación de información en tiempo real y dinámica entre el mundo físico y el mundo de la información. Así que la aplicación de los CPS supervisa y cambia las características del mundo físico autónomo, inteligente, dinámica y sistemáticamente. Hasta el momento se puede deducir que los CPS están más enfocados a la investigación científica, mientras que M2M y el IoT se centran más en la tecnología de la ingeniería y sus productos son más explotables

en los sectores comerciales. Sin embargo en el campo industrial, los sistemas de producción también aceptan y procesan la información alimentada desde el mundo físico mientras manipula el mundo mecánico. La “carga” y “liberación” de la información en el control de la producción tiene un alto grado de sinergia en tiempo real. Entre los tres conceptos de “M2M”, “IoT” y “CPS”, este último se distingue de los demás en que está diseñado para cumplir con esta característica. Por lo tanto, se reconoce como el Internet de las cosas en el campo industrial (IIoT) de última generación (Lee et al., 2015). En resumen, los CPS y los dispositivos que hacen parte del IoT son muy similares ya que comparten la misma arquitectura, y ambos se apoyan en el marco de la comunicación M2M, no obstante, ni los dispositivos IoT ni las comunicaciones M2M presentan una combinación tan alta y coordinación entre elementos físicos y computacionales (Rad et al., 2015).

Numerosos estudios centran sus esfuerzos en un amplio abanico de campos de investigación, sin embargo destacamos el campo sanitario debido a que detectamos ausencia de especialización en algunos sectores. El campo sanitario es tan amplio que los CPS pueden ser usados en un gran abanico de dimensiones tales como la prevención de varias enfermedades o caídas, monitorización de signos vitales, cirugías robóticas (Dolic et al., 2019) o mejora de las capacidades humanas (Sandroff et al., 2018) entre otros.

Según la revisión científica es fácilmente apreciable la alta cantidad de manuscritos dedicados a la salud, sin embargo hemos detectado la ausencia de un sistema capaz de realizar mediciones de memoria bajo un determinado escenario. El escenario al que nos referimos es aquel entorno en el que los usuarios están comúnmente familiarizados, como sus hogares, más concretamente sus cocinas. El sistema propuesto consta de métodos de monitorización no invasiva al usuario y que se vale del mobiliario casero para favorecer la labor. Aparte, no obliga al usuario objetivo a aprender procesos o recordar operaciones para poder usarlo. Gracias a esta línea de investigación, basta y poco explorada, surge el CPS presentando en la actual tesis, de manera que pueda aportar interés y avances científicos aprovechables en este campo.

1.1. Contexto de los sistemas ciberfísicos aplicados a la salud.

Es innegable la asociación de los sistemas CPS y el concepto de la industria 4.0 (Lee et al., 2015), la cual vaticina una hipotética cuarta revolución industrial liderada en gran medida por las tecnologías de la información y la inteligencia artificial. Esta futura tendencia pretende ser el modelo de las futuras fábricas inteligentes, las cuales aumentarán su adaptabilidad a las necesidades y a los procesos de producción, así como a una asignación más

eficiente de los recursos. La ingente cantidad de recursos destinados a este futuro modelo de industria no es ajena al campo de la salud, la cual se nutre bastante de este modelo y que con ayuda de los CPS transforma las herramientas en favor del bienestar y cuidado de los usuarios y ciudadanos de a pie, dando un rol protagónico a aquellas personas con dificultades sanitarias, problemas de salud o con una necesidad exigente de cuidados.

Actualmente se puede evidenciar como muchas personas pueden beneficiarse de los CPS, por ejemplo en los casos que los CPS sirven como sistema de monitorización y alarma para personas mayores o con movilidad reducida. Estos pueden avisar ante cualquier cambio de estado del usuario como puede ser una caída, una variación brusca de la frecuencia cardiaca o presión arterial. En otros casos los CPS están destinados a la detección de síntomas de posibles enfermedades que puedan desarrollar los usuarios. El desarrollo de determinadas enfermedades necesitan de monitorización y control a lo largo del tiempo, ya que estas por su naturaleza no pueden ser apreciadas de forma inmediata. Enfermedades como el Alzheimer no tienen cura, pero un tratamiento a tiempo puede ayudar a paliar y mejorar la calidad de vida de los padecientes. Estos sistemas con las características adecuadas pueden llevar a cabo tal labor sin interferir demasiado en la rutina de los usuarios.

Es inevitable pensar que para todo este rastreo y recopilación de información se requiere una gran infraestructura que garantice el análisis de datos y la fiabilidad de estos. Es aquí donde el IoT entra en juego. Hasta hace unos años el uso de Internet era exclusivamente de los ordenadores, pero con el transcurrir del tiempo este uso se ha ido compartiendo con más dispositivos, el ejemplo más representativo es el smartphone que es usado a diario para realizar operaciones y transacciones. Sin embargo, hoy en día muchos objetos cotidianos pueden estar interconectados a través de Internet haciendo que circule información de nuestro entorno, como refrigeradores que realizan compras, asistentes de voz, pulseras que recopilan información y la comparan o termostatos inteligentes. Al ser objetos cotidianos, su uso pasa casi inadvertido permitiendo, por un lado, la correcta recopilación de datos y por otro la comodidad de los usuarios en no reaprender a usar estos objetos. Debido a la popularización de estos sistemas nacen términos como smart cities, smart homes, smart cars etc, en la que el concepto es el mismo, pero cambia el protagonista, como son las ciudades, las casas o los coches.

Las smart homes u hogares inteligente actuales se caracterizan por brindar funciones en el ámbito del entretenimiento, confort, sostenibilidad y eficiencia energética a los usuarios, sin embargo la salud es un campo que difícilmente se logra saciar dada todas las variantes donde la tecnología puede ser aplicada y extendida. Este territorio que actualmente se encuentra en “alza” por la comunidad científica pretende usar los mismos elementos que los campos an-

teriormente mencionados pero apuntando al bienestar común. Los elementos de mobiliarios de un hogar se destacan por el uso pasivo que se realiza de cada uno de ellos, es decir una cama, un sofá o un armario no son elementos que se hayan de configurar, personalizar o incluso encender o apagar, son elementos en los cuales su uso es muy básico, en un sofá alguien se sienta, en una cama alguien se tumba o un armario es abierto por alguien. La trascendencia de estos elementos en la salud sería su uso desapercibido para la recopilación de información y tratado de esta misma. En este aspecto hemos detectado una carencia como la falta de un mueble que permita el monitoreo del usuario y que prescindiera de algún dispositivo vestible sobretodo para que actúe de manera desapercibida, carencia que esta tesis pretende cubrir. Una hipotética cama con un CPS podría ofrecer el índice de masa corporal (IMC) de un usuario para que este pueda regular su actividad física y alimentación en base al valor del IMC, ya que tal como apunta su definición las personas con sobrepeso tienen una probabilidad de morir similar a las personas con peso normal, mientras aquellas personas “obesas” o “por debajo de lo normal” tienen un probabilidad mayor de morir (Flegal et al., 2005).

En cuanto al consumo energético y desde el punto de vista lucrativo, un CPS es un sistema que está añadiendo un consumo extra a la factura periódica del usuario. Sin entrar a valorar cuántos céntimos de más cuesta nuestra salud, es evidente la percepción de un incremento energético, por lo que la eficiencia energética presenta un peso moderado en la puesta en marcha de un CPS. Cada vez que se habla de eficiencia energética, se habla de cómo usar inteligentemente la energía, para ello se debe reducir su consumo sin que afecte a la calidad de vida.

Día a día se consumen toneladas de energía, durante todo el día e incluyendo la noche. Campos como la industria, la minería, los medios de transporte y el comercio usan energía en todos sus procesos. Por lo que si nos remitimos a la definición más primitiva de energía como: “capacidad de los cuerpos o conjunto de cuerpos para efectuar un trabajo” vemos que es uno de los aspectos más importantes, ya que la energía mueve el mundo. La electricidad se transforma en frío, el gas se convierte en calor, el petróleo se transforma en movimiento e incluso lo que comemos también se transforma en energía. Sin embargo, no siempre estamos ingiriendo alimentos para estar en constante marcha, ya que nuestro cuerpo inteligentemente administra el consumo de alimentos y establece reservas de energía para el momento que le haga falta. De cara al funcionamiento de un CPS, esta es la filosofía que más resulta interesante, ya que es probable que no se requiera del uso del CPS constantemente y en todo momento, al menos no de todas sus funciones. Indagaciones que más adelante serán detalladas evidenciaron la ausencia de un modelo energético que se adapte a la rutina del usuario, por esta razón el enfoque propuesto va acompañado de un modelo de eficiencia energética

basado en comunicaciones verdes (Abrol y Jha, 2016) y que ha sido testeado en una pulsera inteligente para medir la frecuencia cardiaca del usuario, con el fin de suplir esta carencia en la literatura. Trabajos como el anteriormente mencionado, son los que dan como resultados los beneficios de la eficiencia energética (Kaur y Sood, 2015). Estos beneficios incluyen la disminución de la dependencia de otros países por fuentes energéticas, ahorro, ya que al reducir el consumo se gasta menos, reducción de la presión por los recursos naturales para producir energía y una contribución directa a la reducción de gases de efecto invernadero que inciden directamente al cambio climático.

En los CPS, especialmente en los dedicados a la salud, la seguridad es un elemento crítico, ya que información sensible podría quedar desvelada, o el sistema podría quedar bloqueado mediante un ataque o un ciberataque evitando que se produzcan alarmas de vida o muerte, críticas o innecesarias. Por ejemplo si se está apunto de sufrir un infarto y el sistema no lo detecta por un ataque informático, las consecuencias podrían ser desastrosas. Estos ataques no solo afectan de esta manera, en otros ámbitos afectan a la reputación de una empresa o producto convirtiéndolo en algo poco fiable, y también inciden sobre pérdidas con cifras cuantiosas (Arora et al., 2011) de las que muchas pymes no pueden recuperarse. Para los CPS es aconsejable un sistema bien diseñado sin carencias tecnológicas, a veces basta con algo tan básico como un cortafuegos o antivirus y routers configurados de manera segura. Además, hay otras medidas que pueden suponer algo de más coste, pero que son igualmente necesarias como la elaboración de un plan de seguridad que consiste en identificar los datos importantes para que sean protegidos, medida que normalmente va asociado a la contratación de un especialista.

Existen muchas alternativas para gestionar los ataques, pero también existen muchos tipos de ataques. Una de las primeras cosas que inciden en la ciberseguridad es la anticipación, sin embargo durante el estudio de los CPS queda evidenciado que este es un campo muy amplio para ser totalmente abarcado. Además, ha dado pie a ser investigado en abundantes ocasiones y estudios como el de Khattak et al. (2019) allanan el camino para elaborar medidas de seguridad para los CPS y sus componentes, además de permitir el desarrollo de herramientas que permitan actuar anticipadamente. Un simulador basado en agentes, como el que más adelante se detalla, es la herramienta propuesta para anticiparse al comportamiento de los atacantes, de esta manera se puede adoptar las estrategias de defensas más adecuada contra ciertos ataques, a la par que se rellena una insuficiencia en la literatura de la que muchos científicos pueden sacar provecho.

Finalmente, un campo que tampoco se debe obviar es la interacción con los CPS ya que esta interacción puede variar en función de la naturaleza y

la función del sistema. Con el paso del tiempo la tendencia a interactuar con cualquier tipo de sistema, es que esta sea sencilla e intuitiva para ello los sistemas y aplicaciones, no solo los CPS, están diseñados basándose en determinados criterios. En el campo de la informática los criterios de la interacción persona-ordenador (IPO) tienen en cuenta disciplinas como la ingeniería del software ya que esta se basa en metodologías y principios para desarrollar software de calidad lo que implica que entre los requisitos de calidad se incluya la facilidad de uso y la usabilidad, principalmente en las interfaces gráficas para el usuario. Atendiendo a estos ideales una de las partes de las que se compone esta tesis, es la de aportar una aplicación intuitiva y usable para la configuración del CPS, basada en un procedimiento para establecer prioridades en sistemas IoT.

1.2. Contribución de los sistemas ciber físicos aplicados a la salud.

En esta tesis se ha trabajado sobre CPS aplicados a la salud, en concreto se ha trabajado con un mueble inteligente y novedoso como lo es un armario inteligente de cocina capaz de medir la memoria. Este armario se ha usado para cuantificar las pérdidas de memoria con el fin de diagnosticar posibles casos de Alzheimer. Esto es especialmente útil en personas mayores que requieren cuidados constantes. La ventaja de este CPS es que no requiere ninguna actividad explícita por parte del usuario, por lo tanto la medición de la memoria se realiza de manera implícita con el uso del armario. Esta es una de las ventajas frente a los tests para valorar el estado de la memoria hecho por un neuropsicólogo o experto en la materia. En muchos casos se efectúa una valoración del paciente sobre su estado y si este es correcto o adecuado puede ocurrir que la siguiente valoración ya se de por voluntad propia del paciente haciendo que el test quede relegado al olvido y se pierda el seguimiento por parte del profesional.

Como se ha mencionado antes, la diagnosis se realiza mediante la interacción natural del usuario con el sistema, esto conlleva a que el usuario objetivo prescindiera de dispositivos vestibles o wearables para satisfacer los requisitos prescindibles para tal acción. Interacciones simples como la mencionada facilitan la adherencia por parte de los usuarios, requisito al que le hemos dado mucha importancia teniendo en cuenta quienes son los usuarios que se van a beneficiar. En relación a la interacción con el sistema, esta tesis propone una manera alternativa de interacción a la tradicional, esta está basada en el perfil del usuario que interactúa con el sistema. Somos conscientes que muchas personas mayores se encuentran en residencias, centros de días o bajo la atención de un cuidador o familiar, que posea conocimientos técnicos básicos del uso de aplicaciones. Así que introducimos una aplicación que permite es-

tablecer preferencias a la vez que permite establecer la configuración del CPS.

Otra característica del CPS propuesto y que introduce esta tesis es el gasto energético que pueda generar. Aunque los componentes que forman la actual propuesta no generan un gasto alarmante, tenemos en cuenta que un dispositivo de tales características da pie a ser ampliado con más servicios y estos conlleven un gasto adicional. Dado que un mueble no requiere las 24 horas de uso presentamos un modelo energético, el cual atiende a las necesidades horarias del usuario, de tal manera que este se encuentra a pleno rendimiento en las franjas horarias que necesite el usuario. El modelo energético tiene como función principal la eficiencia energética, por lo que el consumo de energía siempre se adaptará al usuario y a sus necesidades, logrando una adaptación a los cambios de franjas horarias del usuario.

En el campo de la seguridad, los principales requisitos en cualquier sistema son la integridad, que se encarga de asegurar que los datos sean fiables. La confidencialidad para que los datos no sean compartidos con usuarios no autorizados y la disponibilidad para que el sistema sea accesible y pueda atender a todas las demandas producidas. Todas estas características son repercusiones de ciberataques, por lo tanto dentro de esta tesis hemos querido contribuir en el desarrollo de medidas de protección para una de las principales vulnerabilidades actuales de estos sistemas, los ataques de denegación de servicios distribuidos (DDoS). Dado que este es uno de los ataques mejor conocidos y que se produce con alta frecuencia (Khattak et al., 2019) se ha decidido trabajar sobre ello. Cabe señalar que el primer ataque de DDoS ocurrió en los años 90 (Steurer y Srivastava, 2003) por lo que es un tema que lleva trascendiendo al menos 20 años y sobre el cual se ha investigado arduamente. A pesar de que ya se han estudiado muchas maneras de prevenir ataques, nuestra contribución parte del desarrollo de un simulador que nos permita configurar estrategias de ataques y probar defensas en sistemas como el actualmente presentado. Esta tesis propone un simulador basado en agentes que permite simular estrategias de ataques DDoS y estrategias de defensas, estas podrían permitir que los servicios de salud relacionados con los CPS se protejan frente a este tipo de ataques y establecer el flujo de información remota de una manera segura.

1.3. Conclusiones de la introducción

Los CPS son sistemas que actualmente se están utilizando en determinada medida en el campo industrial y automovilístico permitiendo la ya mencionada industria 4.0 (fabricación por procesos muy automatizados). Dado que estos sistemas van a estar en el futuro integrados con la vida diaria de cada persona, auguramos un futuro prometedor a la popularización de es-

tos mismo, pero a falta de llegar a ese futuro, debemos hacer frente a los grandes desafíos que presentan los CPS a un nivel más íntimo. El introducir un componente tecnológico avanzado en las rutinas diarias de las personas va ligado a enfrentarse a problemas de seguridad y privacidad que incapacitan las prestaciones de los CPS. Además, aunque estos sistemas son bien acogidos por una gran parte de la población, existe otra más afín a sistemas tradicionales que se niegan a adaptarse a nuevas tendencias, ya sea por falta de motivación, ausencia de ganas de aprender o sistemas de interacción innecesariamente complejos. Dado que los CPS pueden ser explotados en muchos campos esta tesis no pretende dar una solución en cada uno de ellos, pero si pretende exponer y ser punto de apoyo a la comunidad de investigadores que dedican su labor y esfuerzo a integrar los CPS en el campo de la salud.

Este documento, de acuerdo a la normativa vigente, expone una introducción al trabajo realizado. La sección 2 realiza una revisión al estado del arte relacionado con los CPS. La sección 3 plantea el objetivo general de la tesis, y las barreras que han tenido que ser analizadas para lograr las metas deseadas. La sección 4 expone la integración de los artículos publicados y cuáles han sido las aportaciones para lograr el objetivo general. La sección 5 expone las conclusiones obtenidas de esta tesis al igual que argumenta las posibles vías de trabajo futuro teniendo siempre en el foco de atención los CPS y la salud. Finalmente la sección 6 incluye los artículos que componen el núcleo de la presente tesis doctoral.

Capítulo 2

Estado del arte

Los CPS como una nueva rama emergente en el sector de la ingeniería han inspirado una gran cantidad de proyectos en distintos ámbitos. La comunidad científica está trabajando constantemente con arduos esfuerzos en explorar todas las posibilidades que estos sistemas ofrecen para el bien común. No obstante, el diseño de un CPS conlleva una ingente cantidad de componentes. Esta cantidad de componentes está determinada principalmente por el objetivo del CPS y el campo en el que se desenvuelve. Dado que no detectamos un patrón común para el diseño de un CPS dentro de la literatura científica revisada, presentamos el mapa conceptual de un CPS creado por la universidad de Berkeley en la figura 2.1 y en la figura 2.2. En el mejor de los casos, este mapa engloba de manera muy detallada cada aspecto a tener en cuenta en la aplicación, diseño y concepto de un CPS. El mapa ha sido reorganizado y traducido para facilitar su lectura, este mismo puede ser consultado en su pagina oficial (<https://ptolemy.berkeley.edu/projects/cps/>).

Dada la cantidad de aspectos a tener en cuenta, hemos seleccionado los campos que consideramos más relevantes e imprescindibles para que un CPS se convierta en un producto mínimo viable e indagar sobre ellos. Estos aspectos pasan por el estudio de cómo influyen los CPS en el cuidado de la salud, de manera que podamos saber sobre qué ramas se destacan más, hay más ausencia de información o cómo se comportan ante adversidades tecnológicas derivadas de enfermedades. Aquellos muebles o componentes físicos que podamos encontrar para desplegar un CPS también hacen parte de esta revisión, a la vez que sistemas IoT que estén estrechamente ligados con la enfermedad del Alzheimer. Fundamentalmente, estos dos aspectos indicarán las ventajas e inconvenientes de usar un mueble u otro, y como pueden ser entremezclados con sensores para sacar su máximo potencial y saber afrontar problemas básicos. Finalmente, los campos restantes que destacamos son los que tienen que ver con la alimentación eléctrica y la seguridad. Por un lado el consumo eléctrico es un elemento esencial, por lo que los esfuerzos se centran

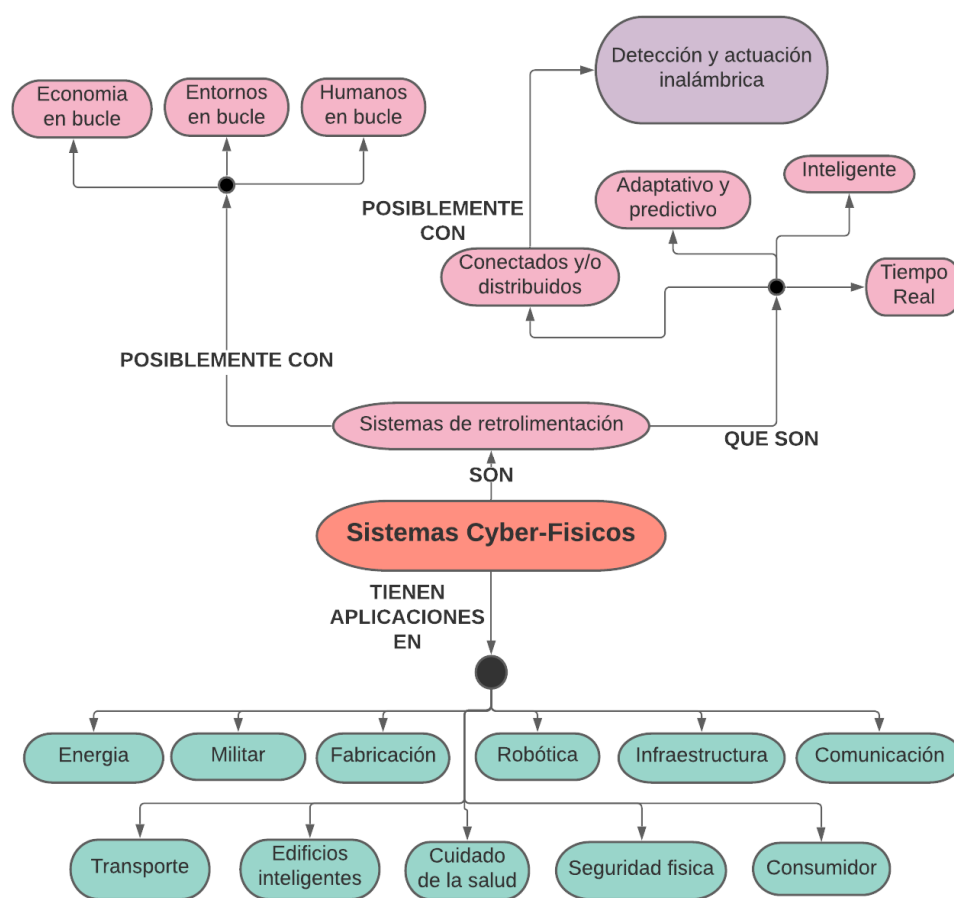


Figura 2.1: Mapa conceptual sobre los CPS. Parte I

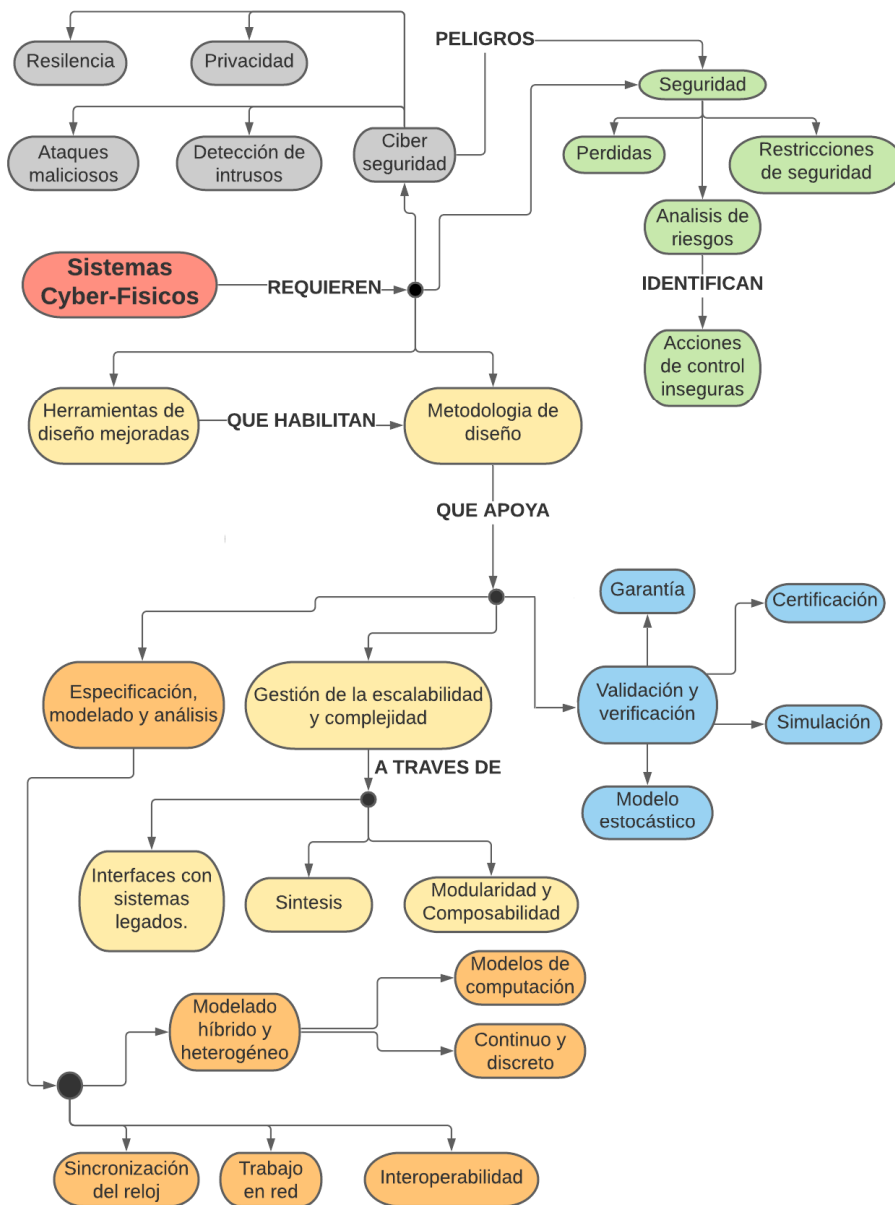


Figura 2.2: Mapa conceptual sobre los CPS. Parte II

en la indagación de modelos de consumo eléctrico inteligente, modelos que reporten un consumo eléctrico adaptativo, enchufes inteligentes o paradigmas que no hayan sido tenidos en cuenta a priori y puedan ser aprovechados. Por otro lado, con el campo de la seguridad intentamos adentrarnos en cuáles son los ataques más susceptibles contra un CPS, maneras que indique la literatura como afrontar dichos ataques, o centrarse en procesos predictivos.

El presente capítulo lista varios proyectos analizados de publicaciones científicas en el contexto del cuidado de la salud, CPS e IoT. Esta revisión del estado del arte ha tenido en cuenta los campos mencionados anteriormente en cuyos lazos con los CPS son estrechos por lo que la estructura del capítulo es la siguiente: La sección 2.1 trata de CPS aplicados a la salud en general, la sección 2.2 comenta aquellos muebles IoT que están destinados al cuidado de la salud, la sección 2.3 lista aquellos proyectos que involucran los dispositivos IoT y la enfermedad del Alzheimer, la sección 2.4 explora otro campo de los CPS de vital importancia como lo es la seguridad, la sección 2.5 lista los proyectos cuyo protagonismo son dispositivos vestibles a cargo de la salud y finalmente la sección 2.6 enumera aquellos proyectos en la que la eficiencia energética destaca.

2.1. Sistemas ciber-físicos aplicados al cuidado de la salud.

En el campo del cuidado de la salud Zhang et al. (2015) abordan el tema de la gestión de la información de un CPS. Este trabajo propone un CPS para aplicaciones y servicios de atención médica centrado en el paciente. En concreto aborda el tema de la estandarización de información para realizar un tratado más eficiente de la información, ya que la información es provista de varios y diferentes dispositivos y de maneras distintas. Otro tema que aborda es el almacenamiento de la información en los CPS, debido a que la cantidad de información que proveen los CPS es alta, los autores proponen usar almacenamiento en la nube y principios de big data para ello. El sistema propuesto recibe el nombre de Health-CPS y su arquitectura está basada en un sistema de capas (capa de recolección de datos, capa de gestión de datos y capa de aplicación de servicios) que permite dar apoyo al problema de la estandarización y almacenamiento de la información.

Lounis et al. (2012) trabajaron en la misma problemática teniendo además en cuenta la seguridad de la información, concretamente proponen una arquitectura propia formada con 4 pilares fundamentales que son: una red de sensores inalámbricos que recolecta información sobre los pacientes, una aplicación de monitorización que permite a los cuidadores acceder a los datos de los pacientes, una autoridad sanitaria que especifica y hace cumplir las

políticas de seguridad de la institución de salud que se hace responsable del paciente y una nube de servidores que aseguran el guardado de datos, además cuenta con un doble sistema de encriptado para proteger la información delicada.

Siguiendo en la línea de los CPS aplicados al cuidado de la salud Haque y Aziz (2013) propusieron un sistema que se enfocó en evitar las falsas alarmas que producen los CPS que monitorean signos vitales. Según los autores las falsas alarmas repercuten en un gasto innecesario de tiempo tanto para los cuidadores como para los pacientes por ello proponen un sistema que realiza el cruce de signos vitales con un conjunto de umbrales para cada signo vital, de manera que un sistema de toma de decisiones clasifica un signo vital cuando este supera un determinado umbral y evalúa otros signos vitales, de tal manera que pueda generar una alarma verdadera.

Chen et al. (2016) trabajaron en un CPS muy particular para el cuidado de la salud, involucrándose en el concepto de ropa inteligente. Su trabajo presenta el diseño de prendas de vestir con material elástico al que se le han añadido varios sensores. La función de los sensores era monitorizar el pulso, la temperatura corporal, actividad eléctrica del corazón (electrocardiograma), miocardio, oxígeno en sangre y actividad eléctrica del cerebro (electroencefalograma). Para el diseño de estas prendas tuvieron en cuenta el material de la ropa, de manera que se pueda generar conductividad eléctrica sin poner en riesgo la vida del usuario y sobre todo que se eviten escollos provocados por toda la red de sensores como insuficiencia de velocidad e interferencias. También propusieron el uso de electrodos secos textiles, para recolectar información del usuario a través del sudor y no suponga una molestia extra para el lavado de la prenda, ya que varios sensores van encajados en bolsillos y deben ser extraídos para el lavado. Los autores concluyeron con una muestra de diferentes programas y aplicaciones para el cuidado de la salud de los parámetros obtenidos con la ropa. Estas muestras consisten en aplicaciones para el cuidado de personas mayores, sistemas fitness, cuidado de las emociones y monitoreo de la actividad eléctrica del corazón para infantes.

Por otro lado, Jassas et al. (2015) desarrollaron un sistema inteligente de monitoreo de signos vitales, aunque su objetivo principal era evitar retrasos en la recepción de la información médica de los pacientes a los proveedores de atención médica. Su principal motivación con este sistema era la de mejorar el tiempo de reacción en las situaciones de emergencia provocadas por accidentes, detener la entrada manual de los datos del paciente y que ésta se efectúe de manera automática, y aumentar la capacidad de camas en caso de catástrofes. La arquitectura del sistema está compuesta por sensores que miden el pulso, el oxígeno en la sangre y la temperatura corporal. Los datos adquiridos por estos sensores son enviados a una Raspberry Pi

(RP), la cual se encarga de clasificarlos y gestionarlos para luego subirlos a la nube. Amazon Web Services (AWS) fue el servicio seleccionado para dar soporte a la computación en la nube, ya que provee herramientas para la escalabilidad del sistema y el tamaño de la datos. El sistema fue probado con simulaciones, de manera que, un programa basado en la toma de decisiones evaluaba diferentes signos vitales y generaba un diagnóstico para el paciente, en el cual avisaba si debía ser ingresado a un hospital o no. Los autores se centraron mucho en el tiempo de respuesta y procesamiento del sistema, de manera que obtenían respuestas, entre la medición de signos y la generación del diagnóstico, de 1 minuto de tiempo aproximadamente.

Finalmente, el trabajo de Majeed et al. (2015) explico el diseño de un sistema de cuidado de la salud móvil. El objetivo principal era reducir la distancia entre pacientes que necesitan cuidados de enfermería a largo plazo y un centro de atención médica. El sistema está compuesto de dos partes una que lleva el paciente y otra por parte de los centros médicos. La parte del paciente consiste en una aplicación móvil y la parte de los centros consta de un sistema central conectado a una base de datos que contiene toda la información de los paciente así como a los centros que está adscrito y toda la información biológica. La aplicación móvil recuerda a los pacientes citas y horas de tomar medicamentos, pero su función principal es la de recibir señales vitales mediante sensores y enviarla a los centros médicos, si estas señales indican anomalía, la aplicación indicará al usuario cual es el centro médico más cercano al que puede acudir. A pesar de que los autores no indicaron que sensores han de ser usados o cómo están conectados a la aplicación, la arquitectura del sistema está pensada para extraer los datos de un smartwatch.

2.2. Muebles inteligentes aplicados al cuidado de la salud.

Dado que un CPS implica un soporte físico, en muchos casos este soporte físico está ligado a algún mueble hogareño de tal manera que añade funcionalidades extras a este. Estas funcionalidades pueden constituir estudiar patrones de los usuarios o monitorizar actividades rutinarias que deban ser cumplidas por ejemplo Becker et al. (2009) expusieron en su trabajo cómo han fabricado un cajón inteligente. La función del cajón es monitorizar y registrar los medicamentos que deben tomar las personas de avanzada edad. El “cajón inteligente”, como lo han bautizado los autores, ha sido creado centrándose en personas mayores con algún tipo de enfermedad degenerativa y que con frecuencia olvidan tomarse una medicación en un momento determinado del día. El cajón registra las extracciones, el tipo de medicina y la hora gracias a RFID, de tal manera que los cuidadores pueden llevar y consultar

un registro de lo que ha tomado un paciente y en función de ello tomar las respectivas correcciones si procede.

Por otro lado Bleda et al. (2017) aprovecharon el uso de una estación ambiental inteligente (unidad capaz de procesar patrones y tomar decisiones) para establecer un ambiente idóneo en el cual se despliega una red de sensores inalámbricos para poder medir diferentes características del ambiente y proporcionar información sobre este, de tal manera que se pueda evaluar las condiciones necesarias de habitabilidad en personas mayores. La red de sensores está desplegada a lo largo de una habitación e incluso debajo del tapizado de algunos muebles y puede medir la temperatura, el peso, el nivel de actividad/movimiento y humedad del usuario. Como mueble inteligente destacan un sillón el cual lleva incorporado un termistor en uno de sus reposabrazos con la intención de detectar la temperatura actual del usuario. Aunque los autores señalan que no es tan preciso como a ellos les gustaría, ya que no puede usarse para un diagnóstico médico preciso, sí que puede dar una estimación de cuando una persona mayor sufre de alta fiebre, o en el peor de los casos puede detectarse un fallecimiento.

Finalmente He et al. (2018) propusieron como mueble inteligente una silla, a la que están anexados dos sensores piezoeléctricos y dos platos de acero para detectar los movimientos del cuerpo de una persona, de manera que la silla funcione como un balistocardiograma. El balistocardiograma es el registro gráfico de los movimientos del cuerpo producidos por la energía liberada por la sístole cardiaca para medir la frecuencia cardiaca. Los sensores piezoeléctricos están situados en los platos de manera simétrica de tal forma que se pueda capturar las vibraciones del cuerpo en forma de señales eléctricas. Según las pruebas efectuadas por los autores el mueble es capaz de medir con alta precisión la frecuencia cardiaca cuando el sujeto permanece inmóvil, de modo contrario, la tasa de fallos al capturar la frecuencia cardiaca es alta, por lo que siguen trabajando en esa línea.

2.3. Internet of things aplicado al Alzheimer.

Los CPS se caracterizan por adoptar muchos elementos del IoT para poder llevar a cabo sus procesos, análisis y fabricación de respuestas (Hatzivasilis et al., 2017) (Cecil et al., 2019). El estudio de los CPS para el tratado de enfermedades neurodegenerativas desde la literatura se ha trabajado en varios ámbitos. El trabajo de Varatharajan et al. (2018) expone un wearable incrustado en las zapatillas para detectar el Alzheimer. Según los autores, un wearable es incrustado para estudiar los movimientos de personas de manera continua. Los patrones de las zancadas provistas por individuos con la enfermedad del Alzheimer son analizados y recolectados, de manera que

luego puedan ser comparadas con zancadas de individuos que no padezcan la enfermedad. La velocidad de la caminata y las zancadas a través del tiempo son analizadas con ayuda de un algoritmo dinámico de deformación en el tiempo (DTW, Dynamic Time Warping en sus siglas en inglés). Este trabajo demostró la efectividad del wearable con algoritmos dinámicos de deformación para una detección del Alzheimer en escenarios primerizos.

Aljehani et al. (2018) presentaron una aplicación realizada en iOS, para ayudar al cuidado de personas mayores que sufren Alzheimer. Se trata de una aplicación que recolecta datos de signos vitales del paciente, a la vez que establece alarmas para diferentes actividades que puede tener el paciente, como tomar una medicación, una ducha, o comidas, además de esto cuenta con una galería de seres queridos del paciente. El proyecto consta de dos partes, una de ellas es la aplicación que usan los cuidadores o familiares del paciente y la otra un smartwatch que debe llevar el paciente en todo momento.

En la línea del IoT se destaca también el trabajo hecho por Ishii et al. (2016) ya que su enfoque presenta similitudes con el de la presente tesis, los autores desarrollaron un sistema para detectar la demencia con la ayuda de una plataforma IoT y la comunicación M2M. Los autores distribuyeron sensores en puntos estratégicos del hogar, como por ejemplo en el grifo del agua, la cocina, pasillos, habitaciones o duchas. Cada sistema de sensores estuvo compuesto por una placa de arduino con un correspondiente sensor dependiendo de lo que se quería medir, por ejemplo, sonido, presión o movimiento, de manera que se pueda saber si un usuario se ha dejado un grifo abierto, deambula a mitad de la noche, va a una misma habitación varias veces u olvida tomar una ducha o toma muchas duchas seguidas. Toda la información acumulada por las placas de arduino son enviadas a un Raspberry la cual se encarga del análisis de los patrones, teniendo en cuenta el tipo de información y a la hora que se ha producido. Los autores han hecho pruebas con pseudo pacientes obteniendo resultados muy satisfactorios. Su siguiente paso es el de instalar esta tecnología en casa de auténticos pacientes con Alzheimer y tomar decisiones en función de los experimentos.

2.4. Seguridad en sistemas ciber-físicos.

La seguridad es otro aspecto fundamental en los CPS ya sea por que los componentes físicos puedan ser estropeados o alterados y el componente software pueda ser intervenido con malas intenciones o por que afecte al funcionamiento del sistema. Dado que algunos CPS tratan información personal es crucial que esta no sea destino de agentes dañinos, por lo que es conveniente una revisión de este aspecto en la literatura. Li et al. (2019) propusieron métodos de aprendizaje estadísticos para detectar comportamientos o señales

anómalas en dispositivos IoT. Para determinar comportamientos anómalos se analizaron datos como ciclos de CPU o uso de disco. Los datos han sido obtenidos gracias a APIs de IoT. Los autores usaron diferentes técnicas de machine learning para poner a prueba sus métodos de tal manera que pudiesen comprobar la fiabilidad y detección de ciberataques o comportamientos indeseados. Concluyeron de su experimentación que las técnicas de machine learning y aprendizaje estadísticos son efectivas para la detección de ciberataques.

Khattak et al. (2019) realizaron un riguroso análisis de los principales ciberataques que se pueden llevar a cabo en la capa de percepción de los dispositivos IoT (la capa de percepción, según Sethi y Sarangi (2017), es donde se encuadran los diferentes sensores encargados de recoger información del entorno, dicho de otra manera es donde los sensores “sienten” los parámetros físicos, o bien se identifican otros dispositivos inteligentes del entorno). La clasificación de los principales ataques la han realizado teniendo en cuenta las siguientes características: autenticación, confidencialidad, integridad, disponibilidad, seguridad de las comunicaciones, no repudio y control de acceso. Los autores concluyen su investigación destacando que los identificadores de radiofrecuencia y redes de sensores son los componentes más importantes en cuanto a la seguridad de la capa de percepción ya que son los más sensibles a ciberataques.

En el trabajo de Kumar et al. (2017) también recayó como responsable de la seguridad, la capa de percepción. Sin embargo, este trabajo centró sus esfuerzos en los microcontroladores del sistema, ya que para los autores son elementos fundamentales en la seguridad al ser robustos a los ataques. El trabajo también reseña brevemente los posibles ataques que puede sufrir la capa de percepción y propuso soluciones que pueden adoptar futuramente los fabricantes de microcontroladores para evitar ataques indeseados.

Stanek y Kencl (2011) desarrollaron SIPp-DD, una herramienta para generar ataques de inundación de protocolo de iniciación de sesión (SIP por sus siglas en inglés) DDoS de tipo real. La herramienta ha sido desarrollada para ser aplicada en las comunicaciones de voz sobre IP y el protocolo SIP. También permite la opción de falsificar direcciones IP de origen y puertos de los mensajes generados, además para mayor flexibilidad se puede ingresar cualquier conjunto de direcciones IP y puertos de origen mediante un fichero de texto. En la fase de prueba se han usado los ataques DDoS disponibles públicamente para demostrar la aplicabilidad de la herramienta. La principal contribución de los autores fue presentar una herramienta adecuada para generar ataques y mediante la simulación obtener los datos adecuados para generar las contramedidas más oportunas.

El trabajo de Anwar y Malik (2014) es destacable ya que se centran en cómo los ataques DDoS pueden afectar a componentes físicos. Concretamente se dedicaron al estudio de las consecuencias que puede tener un ataque sobre los centros de datos con miles de servidores. Los autores partieron de la hipótesis de si un ataque era capaz de derretir equipos o sistemas hardware que estén alojados en habitaciones con mecanismos de ventilación remota administradas por protocolos web y su vez estos protocolos pudieran ser vulnerados. A pesar de que no detallaron exhaustivamente sus simulaciones, aportaron las principales características de estas como las dimensiones del centro de datos, el sistema de refrigeración usado, los elementos de red y el tráfico de datos. Las simulaciones involucraron ataques DDoS tanto a los propios servidores como al sistema de red que gestiona la ventilación, logrando un rápido ascenso de la temperatura. Retomando su premisa, no fueron capaces de derretir ningún sistema, pero sí de generar bastante daño, y a pesar que estos no se pudieron cuantificar ya que se producían en cascada, si que pudieron estimar que 16 minutos fueron suficientes para causar daño. Concluyeron con que aunque las simulaciones fueron muy extenuantes, muchos de los problemas pueden ser solucionados mediante intervención humana.

Finalmente analizamos el trabajo de Antonioli y Tippenhauer (2015) ya que su enfoque se acerca bastante al trabajo presentado. Los autores han desarrollado MiniCPS el cual es una extensión del simulador Mininet. Este simulador se encarga de emular redes mediante software manteniendo el realismo de forma virtual. Los creadores de MiniCPS indican que los CPS del mundo real a menudo no están abiertos a las investigaciones en materia de seguridad en especial cuando tratan de abordar la capa física, motivo que les llevó a crear la extensión MiniCPS. El objetivo principal era crear un entorno de investigación extensible y reproducible para comunicaciones de red, sistemas de control e interacción de la capa física de los CPS. Mininet se encarga de proporcionar una emulación de red en tiempo real con componentes típicos de CPS y controladores lógicos programables mientras que MiniCPS define una api para simular interacciones con la capa física. A pesar de que es un enfoque bastante novedoso y atractivo para la investigación no cubre los conceptos de ataques de DDoS que también pueden afectar a la capa física, por lo tanto la tarea de evaluar estrategias de defensas contra estos ataques recae en una investigación aparte o más extensa.

2.5. Dispositivos inteligentes

Existe una multitud de dispositivos inteligentes o gadgets en el mercado, cuyo objetivo es automatizar muchas de las tareas diarias, incrementar la calidad de vida y el rendimiento de salud. Algunos de los dispositivos comerciales que ya pueden ser usados por el público constan de robots as-

piradores, termostatos, bombillas, cerraduras o asistentes virtuales. En la literatura científica podemos encontrar el trabajo de Sogi et al. (2018) en el que desarrollaron un sistema IoT que tiene como objetivo principal velar por la seguridad del ciudadano. Aunque el usuario principal de este sistema son las mujeres, los autores revelaron que también pueden hacer uso de este chicas pequeñas o adultos mayores. El sistema que desarrollaron se llama SMARISA, el cual trata de un anillo inteligente que posee un botón que debe ser pulsado en situaciones de peligro. Este botón eleva una señal de alarma que pone en marcha un protocolo de seguridad, el cual consiste en recoger las coordenadas sobre dónde se está efectuando la agresión, hacer sonar una sirena, realizar un aviso a un cuerpo de seguridad y tomar fotos de los alrededores. SMARISA está formado por una Raspberry Pi Zero, un módulo de cámara Raspberry Pi y un zumbador o timbre. Los autores concluyeron destacando la eficacia del sistema, sin embargo señalaron que el proyecto es un prototipo funcional al que le faltan ciertos módulos ya que uno de los principales inconvenientes es que este sistema depende mucho de una aplicación móvil y por lo tanto hay una dependencia que debe ser eliminada.

En otro estudio realizado por García-Cruz et al. (2018) se exploraron los potenciales beneficios del uso de smart glasses, concretamente el modelo Google Glass. El estudio invitó a 80 urólogos a usar Google Glass en sus prácticas quirúrgicas y clínicas diarias, para posteriormente puntuar la utilidad de estos dispositivos. Los resultados que se obtuvieron indicaron que las aplicaciones consideradas más prometedoras son aquellas que proyectan videos en tiempo real, reproducen imágenes estáticas, hacen uso de la realidad aumentada, facilitan una navegación laparoscópica y aquellas que ayudan a realizar una comprobación de elementos de seguridad. Los autores concluyeron con la identificación de las diversas utilidades, sin embargo afirman que son necesarios más estudios para abordar las posibilidades y limitaciones reales, con el fin de realizar un uso seguro de estos dispositivos en la práctica.

Siguiendo la línea de dispositivos inteligentes Lee y Chung (2009) diseñaron una camiseta inteligente que medía la actividad eléctrica del corazón, lo que comúnmente se conoce como electrocardiograma, y las señales de aceleración del corazón en tiempo real. La camiseta está compuesta por una red de sensores inalámbricos, telas conductoras y un acelerómetro para garantizar el continuo monitoreo y obtención de señales del cuerpo como si las estuvieran extrayendo electrodos. Como características adicionales el sistema ha sido diseñado para poder ajustarse perfectamente a una camiseta y de bajo consumo eléctrico. La camiseta inteligente ha sido probada por varios voluntarios en un andador a velocidades entre 5 y 8 Km/h obteniendo resultados muy favorables. Los autores concluyeron indicando que sus expectativas habían sido alcanzadas y que ahora seguirán trabajando en la precisión de este sistema para poder realizar diagnosis.

Abu-Faraj et al. (2012) diseñaron un prototipo de calzado guía para personas ciegas. En este sistema, cada zapato posee tres pares de transductores ultrasónicos (transmisor y receptor) situados en el centro, lateral y en la parte media superior del zapato. La función de estos elementos es la detección de obstáculos, agujeros u hoyos que puedan ser encontrados a lo largo del camino. Según describen los autores, los transductores logran detectar obstáculos a unos noventa centímetros alrededor del usuario. Además de los zapatos, el sistema también está compuesto por gafas que también incluyen transductores para detectar obstáculos a la altura de la cabeza. En totalidad el sistema está alimentado por una batería de 12 V y 2500 mAh y las señales están gestionadas por un microcontrolador ubicados en el cinturón del usuario. Tras las pruebas de validación del sistema los autores concluyeron que debían seguir mejorando en algunos aspectos del sistema, como la sujeción de los sensores y una calibración de estos mismos antes de ponerlo en marcha en condiciones reales. Aunque este sistema no se dedique a la monitorización de señales vitales, se dedica a la vigilancia del usuario mediante sensores, característica que lo hace destacable para medir el alcance de los dispositivos inteligentes dedicados a mejorar la calidad de la vida.

El-Nahas et al. (2018) llevaron a cabo un estudio pionero que han denominado smart socks o calcetines inteligentes. El objetivo de esta investigación era demostrar la relación entre la alta temperatura del pie con la aparición de una infección denominada pie diabético, para ello evaluaron unos calcetines capaz de medir la temperatura y la presión plantar. Los calcetines inteligentes poseen siete sensores térmicos tejidos en la tela, los cuales están conectados a una unidad central que gestiona los cambios de temperatura. La presión plantar ha sido medida por un sistema de terceros denominado MatScan. Los resultados de sus pruebas dieron varias conclusiones dispares, como que no eran necesarios siete sensores para realizar todo el estudio, sino simplemente dos. Por otro lado, consideran usar otro tipo de sensores, especialmente más baratos, para medir la humedad en los pies ya que también puede estar relacionado con el pie diabético. Aunque no pudieron determinar relaciones entre la temperatura y la infección, los autores comentan que si se enfocan en el calor, la humedad y otros factores posiblemente podrán obtener resultados prometedores.

Finalmente, la investigación de Nam et al. (2016) cuyo esfuerzos se centraron en crear un cinturón inteligente. La principal motivación es corregir la postura de los usuarios para reducir la obesidad abdominal, ya que puede repercutir en fallos cardiacos, diabetes y alta presión sanguínea. El dispositivo consta de un sensor de fuerza y un sensor de aceleración, fundamentalmente para detectar la presión abdominal entre el cinturón y el abdomen del usuario y por otra parte distinguir cuando el usuario está de pie o sentado

y erguido o sentado e inclinado. Los resultados de las pruebas corroboraron cual es el mejor sitio para situar los sensores en el cinturón, además de la precisión de los sensores para detectar la postura en la que se encuentra el usuario. Los autores concluyeron que partiendo de estos resultados se enfocarán en desarrollar un sistema de retroalimentación para indicar al usuario cuando debe corregir su postura.

Somos conscientes de que el sistema presentado en esta tesis no contempla el uso de dispositivos vestibles o wearables, de hecho, es una de las características principales, que el usuario no disponga de ninguno de estos elementos. Sin embargo, consideramos que es importante el estudio de este tipo de dispositivos para ampliar nuestro punto de vista y ampliar más el conocimiento sobre el alcance al que pueden llegar las características de estos dispositivos. Dado que estos dispositivos pertenecen al sector IoT y nuestra propuesta se nutre de este campo, surge la propuesta de una de las principales singularidades del CPS. Como se verá más adelante el estudio hecho con ayuda de una pulsera inteligente dio como resultado el modelo energético propuesto para el CPS.

2.6. Eficiencia energética

Como indica el trabajo de Van Kranenburg y Bassi (2012) la energía será un próximo desafío tecnológico en los siguientes 5 a 10 años en lo que se refiere a IoT, por lo tanto se sugiere realizar más investigaciones para desarrollar sistemas capaces de recolectar energía del medio ambiente, evitar desperdicio de esta, efectuar un uso inteligente o adaptativo de esta, o emplear esfuerzos en crear sistemas capaces de gestionar estrategias de ahorro en función del sistema que se esté alimentando. La sección actual realiza una revisión de varios proyectos en la literatura científica cuyo eje común gira en torno a las técnicas para realizar un uso eficiente de la energía en los CPS e IoT.

El trabajo de Moreno et al. (2014) consiste en el desarrollo de un sistema de ahorro de energía para edificios residenciales y comerciales ya que el consumo de estos está entre un 20% y un 40% de la energía total en los países desarrollados. Para desarrollar tal sistema se desglosó en áreas separadas las zonas de un edificio, de esta manera los principales parámetros que afectan al consumo energético pudieron ser analizados. El análisis permitió proponer una predicción sobre el consumo diario lo que a su vez dio paso a implementar y diseñar acciones para ahorrar energía. Algunos ejemplos han sido: proponer estrategias para ajustar el tiempo de operación y configuración de los electrodomésticos o dispositivos involucrados y seleccionar la distribución óptima de energía para maximizar el uso de energías alternativas. Para validar el sistema los autores realizaron experimentos en 3 edificios. El primer

edificio constaba de una variedad de comportamientos de los ocupantes. El objetivo de este experimento fue verificar la relación directa entre las condiciones ambientales y los comportamientos de los ocupantes, y la energía eléctrica consumida por los aparatos de confort distribuidos en el edificio. Luego, se infirieron estrategias óptimas para ahorrar energía teniendo en cuenta el efecto de dichos parámetros sobre la energía consumida. Estas estrategias se aplicaron en un laboratorio de pruebas de un segundo edificio, donde se dispuso de un alto nivel de monitorización y automatización. En ese segundo escenario se realizaron experimentos controlados y los resultados mostraron que, luego de aplicar estas estrategias, se podrían lograr ahorros de energía de entre 14% y 30%. Finalmente, y con el objetivo de validar la propuesta de gestión energética de edificios en un escenario más realista con capacidades de monitorización y automatización reducidas, se seleccionó un tercer edificio donde se llevaron a cabo diferentes acciones de ahorro energético. A partir de estas acciones, se logró un ahorro energético de alrededor del 23%. De esta forma, los autores demostraron la aplicabilidad de su sistema de gestión propuesto.

El green computing o tecnologías verdes, de manera muy breve, se refiere a realizar un uso eficiente de la energía y surgió como una manera de alargar la vida de las baterías que alimentan sensores o dispositivos IoT. Bajo este concepto se desarrolla el trabajo presentado por Arshad et al. (2017), el cual efectuó un análisis y clasificación de proyectos cuyo punto en común es el ahorro y la eficiencia energética. Con este análisis los autores indicaron cuán práctico y posible son cada uno de los enfoques. Destacamos este proyecto porque gracias a él es fácil evidenciar que técnicas son las usadas por la comunidad científica, algunas de ellas son: realizar la adecuada selección de determinados sensores para trabajar, programación modo de bajo rendimiento, asignación de diferentes tareas a diferentes núcleos del sistema, reducción del camino de transporte de datos, uso pasivo de sensores, reciclaje de elementos para hacerlos productivos otra vez, entre otros. Lógicamente no todos estos mecanismos son aplicables a todos los sistemas, así que, ellos son aplicables según la naturaleza del sistema IoT. El objetivo principal de los autores fue proporcionar una determinada serie de reglas o consejos para un correcto uso de la energía y con ayuda del análisis concluyeron que estas reglas son: reducir el tamaño de las redes de sensores siempre que sea posible, realizar un uso selectivo de sensores, usar una arquitectura híbrida, es decir usar sensores activos y pasivos para según qué tarea, formular políticas de ahorro de energía, es decir reglas que todo el mundo debe seguir para ahorrar energía, y finalmente realizar compensaciones inteligentes es decir priorizar de manera inteligente los costes de algunas acciones o situaciones de procesamiento o comunicación para ahorrar energía.

El trabajo de Saifuzzaman et al. (2017) se centra en el desarrollo de un

sistema de ahorro de energía en la ciudades mediante el uso de las luces callejeras. Los autores se basaron en una encuesta (Cho y Dhingra, 2008) de la cual pudieron extraer que en promedio el 30% de la electricidad de una ciudad es consumida por las farolas y otros elementos de alumbrado en la ciudad, de ahí la motivación de su trabajo. Concretamente el trabajo propuso un uso controlado de la electricidad en aquellas vías o avenidas donde no se detecten automóviles y en ciertos horarios, por ejemplo entre la 1 y 6 de la madrugada. El enfoque fue probado con ayuda de una maqueta con sensores de luz, sensores de movimientos y una placa de arduino para el control de estos elementos durante varios meses. Los resultados arrojaron que mediante este sistema se consigue un ahorro de entre el 30% y 40%. Los autores concluyeron que un proyecto de esta magnitud es factible y fiable, por lo que esperan desarrollar una aplicación para el control de la monitorización de las luces. Sin embargo, este proyecto aún ha de ser evaluado ante condiciones adversas y en un escenario real.

El trabajo de Eteläperä et al. (2014) también ha demostrado mejorar la eficiencia energética. La manera en cómo han abordado el tema es mediante la reconfiguración de objetos dedicados a las tecnologías de la información y comunicación (TICs) en tiempo de ejecución con el fin de alargar la vida de la batería de los sensores del sistema. Para probar su modelo de ahorro usaron tres casos de uso con una estación meteorológica al aire libre que funciona con baterías y un conjunto de datos. Los casos de uso consistieron en analizar el gasto energético que se producía mediante la transmisión de datos de la estación a través de una compresión de información parcial, compresión total y compresión con pérdidas. Los resultados obtenidos demostraron que si se re-configura el modo de transmisión de sin compresión a compresión con pérdidas se puede conseguir un ahorro del 47,9%. Sin embargo para que el ahorro compense la pérdida de información se debe usar el método de compresión con pérdidas de 10 a 118 minutos, ya que la pérdida de información puede atribuirse a un error en el muestreo de la información.

En Man et al. (2012) se ha usado un modelo basado en aprendizaje automático (machine learning) que implementa un algoritmo de regresión de bosques aleatorios para predecir la duración de la batería de los dispositivos IoT. Los autores evaluaron su modelo propuesto con un conjunto de datos generados a partir de sensores de una red IoT. En este modelo se usaron varias técnicas de preprocesamiento como normalización, transformación y reducción de dimensionalidad. El modelo propuesto logró una precisión del 97%. Los resultados obtenidos demostraron que el modelo propuesto funciona mejor que otros algoritmos de regresión para preservar la duración de la batería de los dispositivos IoT.

Finalmente, el manuscrito de Maddikunta et al. (2020) en vez de propo-

ner un enfoque novedoso realizó un estudio sobre los métodos tradicionales sobre la estimación del estado de carga de la batería en CPS. Los autores mencionaron que la importancia de estimar correctamente los niveles de batería repercute directamente sobre su ciclo de vida útil, de manera que la estimación pueda evitar sobrecargas o desgastes prolongados debido a la descarga. La conclusión del trabajo es que existe aún un gran espectro para la investigación de este campo y los autores estiman que los enfoques más prometedores irán acompañados de inteligencia artificial y/o métodos formales para la administración dinámica de la energía.

Mediante esta revisión queremos destacar dos puntos que recaen directamente sobre este tema. El primero de ellos es que a diferencia de los otros temas revisados en el presente capítulo este es el que más disperso se encuentra, es decir, la eficiencia energética es un tema candente y que se está aplicando a un variado abanico de sistemas y componentes. El segundo punto es que la comunidad científica está centrando sus esfuerzos mayoritariamente en mejorar las condiciones y características de la conducción eléctrica, lo que unido al punto anterior, evidencia una clara ausencia de investigaciones en los CPS dedicados a la salud. Consideramos que nuestro aporte ayude a llenar esta ausencia y pueda ser aprovechado en sistemas de características equivalentes.

En conclusión, con esta ardua revisión del estado del arte podemos observar cual es la situación actual de los sistemas y sensores cuya relación con los CPS y ámbito de la salud es estrecha, a la vez que se observa las particularidades derivadas. La revisión ha indagado en las áreas de los CPS aplicados a la salud, muebles inteligentes, IoT aplicado al Alzheimer, seguridad y dispositivos inteligentes. Sin embargo, ninguno de estos trabajos permite la monitorización y medición de la memoria a la vez que la pronta diagnosis de enfermedades neurodegenerativas. En este contexto, esta tesis suple esta carencia presentando un armario de cocina inteligente con las funciones anteriormente descritas y prescindiendo de elementos de seguimiento como pulseras o dispositivos inteligentes que repercuten directamente en la comodidad del usuario. Además, le acompañan propuestas en el área de seguridad y el sector eléctrico, concretamente un simulador que permite establecer estrategias de defensa contra ciberataques bien conocidos y un modelo de ahorro eléctrico basado en la rutina diaria que el usuario realiza en casa.

La siguiente sección detalla el principal objetivo que se pretende alcanzar con esta tesis al igual que se detalla todos los subobjetivos en los que se divide y los desafíos que ha supuesto superar para alcanzar el objetivo principal. A la vez se exponen las alternativas que se han sopesado para dar con el concepto final. Finalmente, se exponen todos los elementos definitivos que han conformado el sistema presentado.

Capítulo 3

Objetivos y planteamiento de la tesis

Como se ha descrito en capítulos anteriores, existen muchos sectores en el campo de los CPS aplicados al ámbito de la salud que deben ser indagados poco a poco, la presente tesis no pretende abarcar todos y cada uno de esos campos ya que es un trabajo arduo y debe ser llevado a cabo por toda una comunidad científica. Sin embargo, lo que sí pretende esta tesis es ser punto de referencia con la ayuda de una herramienta que brinde una forma de monitorización latente y no invasiva, de manera que se pueda realizar un seguimiento del usuario a través de una interfaz casi invisible que facilita la interacción sin llevar a cabo un proceso de aprendizaje innecesario y tedioso. El proceso de monitorización se efectuará centrándose en la enfermedad del Alzheimer sin ningún dispositivo inteligente vestible que deba portar el usuario. Con la sección 2.5 es posible apreciar toda la potencial información que se puede obtener a partir de estos elementos, sin embargo queremos ponderar la comodidad y el confort, así que prescindiremos de estos. Dado que los gadgets y wearables juegan un papel importante en el ámbito del IoT queremos aprovechar algunas de sus características para apoyar el funcionamiento del CPS. Dentro del análisis de los dispositivos inteligentes se presenta además un modelo de ahorro energético y además deja entrever la necesidad de un medio de retroalimentación o alarma que indique al usuario que debe hacer ante una determinada circunstancia. Ambos elementos mencionados apoyan las pretensiones de esta tesis y el diseño del CPS.

Este capítulo abarca el planteamiento del objetivo principal de la tesis y aborda todos los desafíos que fueron planteados para llegar a tal objetivo. El análisis de todos los desafíos incluye todos los requisitos e impedimentos que se han desprendido durante todo el proceso de ejecución de manera que la visión global de la propuesta pueda ser entendida mediante una exposición paso a paso.

3.1. Objetivos generales.

El objetivo principal de la tesis es ofrecer un CPS aplicado a la prevención y diagnóstico de enfermedades, a través de interfaces “invisibles” y usables, en concreto nuestra investigación se centra en el control de enfermedades neurodegenerativas. Llamamos interfaces invisibles a la manera o proceso que tiene nuestro sistema para recoger datos del usuario y procesarlos con una mínima interacción, ejemplos recientes nos remiten al pago con tarjeta usando la modalidad de contactless o el uso de asistentes de voz como Alexa o Google Home. Concretamente esta interfaz solo se limita al uso natural del CPS, por lo que en principio solo bastaría la interacción natural del usuario para poder poner en marcha el proceso de diagnóstico.

A pesar de que el objetivo principal está claro, debemos descomponerlo para poder exponer todo el abanico de subobjetivos que abarca y a su vez describir poco a poco y en detalle el camino recorrido para llegar hasta el.

En primer lugar hemos podido observar que los proyectos de investigación de enfermedades neurodegenerativas se dividen en dos grupos, a grandes rasgos, el primero de ellos, con una fuerte influencia del sector de la medicina, centra sus esfuerzos en buscar una cura para enfermedades como el Alzheimer. El otro grupo, que es donde nos enmarcamos, se centra en el desarrollo de tratamientos paliativos o sistemas de soporte a pacientes con Alzheimer. Dada estas distinciones, uno de nuestros objetivos es que el CPS sea una herramienta que sirva para la detección de enfermedades neurodegenerativas como el Alzheimer y que sirva de utilidad a personas que padecen dicha enfermedad o corren el riesgo de padecerla y de apoyo a familiares o cuidadores.

En segundo lugar, como objetivo secundario nos hemos planteado que el usuario al que va destinado este sistema pueda hacer uso sin necesidad de tener que leer manuales, o aprender pasos innecesarios. Esto nos motiva a emplear interfaces invisibles, de manera que el uso de este sistema se realiza aprovechando el aprendizaje ya adquirido que tiene el usuario de otros elementos que ya posee. Además, por medio de un uso natural de este e interviniendo de manera invisible en el día a día se puede efectuar el seguimiento y diagnóstico de la enfermedad.

Como tercer objetivo secundario, pretendemos una gran adherencia por parte de los usuarios a nuestro sistema. Debido a que el usuario objetivo de nuestro sistema está definido, no descartamos tratar con usuarios que se encuentren en una etapa avanzada de la enfermedad o usuarios que tengan una incapacidad visual. Esto nos alienta a establecer maneras de interactuar que “faciliten la vida” a estos usuarios, por lo que incorporar una interfaz que mejora la adherencia a las que nos referimos y sea adaptada a este tipo de

usuarios es un tema de mucha importancia.

Gracias al análisis de desafíos e inconvenientes para el desarrollo de un CPS que se ha llevado a cabo queda de manifiesto las principales contribuciones y las áreas que se ven repercutidas. Aunque futuramente serán analizadas, se presenta una breve descripción de estas.

La principal contribución de esta tesis es la de presentar la investigación realizada para llevar a cabo el diseño del sistema de monitorización y la selección de herramientas necesarias para tal tarea. Además, como requisito se introduce la necesidad de un diseño low-cost, fundamentalmente para que este tipo de estudios llegue al usuario de a pie a un coste accesible.

Al margen de la contribución principal se desprenden otras contribuciones menores centradas en el análisis de aspectos de configuración del sistema, en concreto la que encontramos dentro del entorno de las aplicaciones móviles dedicadas a la gestión de prioridades de servicios en sistemas IoT, ya que una aplicación de este tipo es requerida para la configuración del sistema. Esta aplicación fue diseñada para establecer prioridades en servicios 5G, pero ha sido adaptada para el uso y configuración del CPS. Otra contribución menor implica el estudio de componentes físicos sobre donde desplegar un CPS en entornos domésticos. El estudio comprende el análisis de la usabilidad del componente físico al igual de como este puede ser reaprovechado en sistemas de similares características. Además, introduce los requisitos de diseño para la usabilidad de un CPS en función de un amplio espectro de comportamientos que se puedan efectuar, ya que no siempre el usuario objetivo va a tener que enfrentarse a tales sistemas, también incluye a familiares o cuidadores.

Dos áreas más que reciben contribuciones son el área energética y el área de seguridad. Para la primera se ha desarrollado un experimento en el cual se ha tenido en cuenta la rutina diaria del usuario y se ha monitorizado su frecuencia cardíaca con ayuda de una smartband. Gracias a esta monitorización se ha podido establecer un modelo energético en el cual se establecen rangos horarios en la que la smartband se encuentra funcionando a pleno rendimiento. Cuando la smartband no está a pleno rendimiento, está con sus funcionalidades mínimas de manera que sigue monitorizando al usuario en rangos horarios menos riesgosos y se ahorra energía. El modelo energético que ha sido resultado del experimento se extrapola al uso del CPS, de manera que este pueda estar a pleno rendimiento durante las franjas más concurridas por el usuario y en las que no, se produzca un ahorro energético. Sin incurrir en causas excepcionales o personales de cada individuo, es lógico pensar que los momentos más álgidos son justos antes de cualquier comida, y los de menos uso es cuando se está durmiendo, generalmente por la noche.

Finalmente en el área de seguridad la contribución va más enfocada a un simulador que ayude a hacer frente a los ataques DDoS. Este simulador permite enfrentar y probar estrategias de defensa y ataques de DDoS con la finalidad de que se consiga la máxima protección del sistema junto con el proceso de diagnóstico adjunto y que el funcionamiento del sistema no se vea comprometido.

Para llevar a cabo nuestro objetivo principal analizamos los principales desafíos que nos encontramos para diseñar un CPS con las características requeridas. Así que el resto de secciones abordan la fase de análisis de temas en los que más nos hemos centrado como el componente físico adecuado, la interacción de los usuarios con el CPS, el tema de la prevención de las enfermedades neurodegenerativas, el sistema de alimentación y medidas de seguridad.

3.1.1. La elección del componente físico en el CPS.

Dado que el cometido principal de la tesis es ofrecer un CPS, la primera incertidumbre que nace es donde ubicar tal sistema. Dado que el ámbito de trabajo es la salud mediante la monitorización lo ideal sería reutilizar elementos caseros u hogareños para tal fin. En cuanto a los elementos hogareños que un usuario común pueda tener en su casa podemos listar: puertas, mesas, sillas, armarios, camas, ventanas, escritorios, sofás, cajones, mesitas de noche y sin fin de elementos más. El factor común de todos estos elementos es que son objetos con los que el usuario puede interactuar de manera natural, y esto es algo positivo ya que si el usuario prescinde de elementos se seguimiento deberá interactuar con algún componente físico que permita rastrear su comportamiento. Por lo tanto, la decisión del componente físico dependerá de las magnitudes que se pretendan medir, en la facilidad del despliegue del CPS, costes del CPS y frecuencia de uso del componente físico.

Más adelante haremos mucho más hincapié en este elemento, pero desde ya queremos destacar su importancia no por lo que representa, sino, más bien por el ámbito en el que se desenvuelve. Si se diera el caso del diseño de un CPS para entornos industriales y grandes cadenas de montaje, con bastante probabilidad nos centraríamos en que el componente físico fuera usable, dejando atrás otras características de lado, ya que la Industria 4.0 demanda otro tipo de requisitos. Dado que una de las principales diferencias entre el entorno industrial y el entorno casero es la especialización y el conocimiento de los usuarios, la correcta elección del componente físico hará que podamos aprovechar los conocimientos que el usuario ya posee para desenvolverse mejor con este. El usuario no deberá verse involucrado, o no demasiado, en el aprendizaje de un sistema que puede ser innecesariamente complejo si se diseña mal, de ahí radica la importancia de selección de este

elemento.

Hemos mencionado antes el caso de la Industria 4.0 ya que va de la mano con el concepto de CPS, por lo tanto es una obligatoriedad el componente físico (Wang et al., 2011). Cuando se habla de CPS lo normal es pensar en enormes factorías con una elevada cantidad de procesamientos y tareas, en la cual varios componentes o sensores están conectados para sacar adelante un objetivo, esto al menos es así desde el concepto de la Industria 4.0 (Lee et al., 2015). Dado que el presente caso trata un hogar y usuarios convencionales y no especializados en procesos industriales, el CPS debería de estar desplegado sobre un componente que el usuario poseyera en su hogar, y en el mejor de los casos no sobre un objeto que tuviese que adquirir o comprar, más bien algún elemento que ya posea en casa. Así que con estos datos, el primer desafío que plantea esta tesis es evaluar cuál de los elementos que un usuario posee en su hogar es el más adecuado para desplegar un CPS para la monitorización de la salud.

3.1.2. Interacción del usuario con el CPS.

En el ámbito de los CPS el lector debe recordar que este se trata de un sistema automatizado de información y comunicación, cuyo punto de partida para empezar el proceso de automatización y análisis de datos es la capa de percepción, la cual se encarga de recopilar información del entorno y transformar datos en señales digitales. Según la clasificación de aplicaciones de sistemas ciberfísicos (Cardin, 2019) los elementos más usados en la capa de percepción son sensores o identificadores de radio frecuencia. El enfoque presentado tiene en cuenta estos elementos para el diseño del sistema, sin embargo suscita un debate que desencadena el segundo desafío a superar. Partiendo de la idea de que se diseña un CPS enfocado en la salud, la intervención del usuario debe ser obligatoria ya que este debe aportar algo que favorezca la diagnosis, y para ello debe haber un proceso de interacción balanceado que no entorpezca el uso del CPS y este puede llevar a cabo su labor. Así que como diseñadores debemos indagar cuál debe ser el primer paso que debe dar nuestro CPS para el control del usuario, o a lo mejor debemos plantear esta idea desde otro punto de vista, por ejemplo dando por hecho que el usuario debe ser el encargado de poner en marcha el sistema. En la medida que esta duda sea trabajada más en profundidad determinaremos si el CPS debe estar en constante funcionamiento todo el día a la espera del usuario o más bien si el usuario con su acción de actuar provea la suficiente información para dar una retroalimentación óptima. Sea cual sea este punto de arranque, el segundo desafío a superar se plantea y consta de analizar de métodos de interacción que han de ser ofrecidos al usuario.

El análisis de los métodos de interacción nos hace abordar las posibilidades

existentes como aplicaciones móviles, smartwatch, smartbands o asistentes de voz. Incluso puede hacernos replantear algunas ideas preconcebidas si no se ha determinado cual es componente físico definitivo al que debe ser acoplado. Aunque la prioridad está en indagar sobre interfaces invisibles para evitar cualquier dispositivo vestible el análisis abre una gran abanico de posibilidades que pueden apoyar otras características del sistema que giren sobre este mismo eje. Partiendo del desconocimiento de cuan complejo puede llegar a ser la configuración del CPS, una nueva manera de interactuar con el sistema nace aquí, cuyo objetivo principal es pautar la configuración básica que este sistema requiera. Esta otra manera de interacción no es para la cual fue creado el CPS si no para establecer comunicaciones o prioridades en el sistema, y que por supuesto no atañe exclusivamente al usuario objetivo si no también a sus familiares o algún cuidador.

3.1.3. Herramientas de medición.

Desplazando el foco de atención a otros aspectos de los CPS, caemos en la cuenta que normalmente los sistemas de monitorización requieren elementos clínicos, incluso un software y hardware anexo que ayuden a traducir señales. En los casos más extremos se aprecian sistemas formados por camillas, monitores o ventosas y en el lado opuesto, es posible que el sistema esté compuesto por sistemas básicos o poco voluminosos como un tensiómetro. Dado que la actual propuesta va dirigida a un entorno casero, los medios y el hardware elegido deberá ser aquel que mejor pueda acoplarse a este entorno. Esto recoge a todas aquellas opciones hardware que entren dentro del concepto low-cost o que no represente una inversión excesiva, que se ajuste a medidas nada voluminosas con las que el usuario se sienta cómodo. También se priorizará aquel hardware que permita cumplir mejor con la filosofía del diseño centrado en el usuario destacando la mayor satisfacción por parte de este con el mínimo esfuerzo (Abrás et al., 2004).

Los CPS que están dirigidos al cuidado de la salud normalmente están involucrados en la monitorización de signos vitales o de pacientes en concreto. Incluso esto es un hecho latente en los artículos que fueron preseleccionados para la revisión del estado del arte pero que han quedado descartados. Algunos ejemplos de proyectos remarcan la influencia que ejercen los programas estatales en la salud de los niños (Sasso y Buchmueller, 2004) o proponen métodos para almacenar y compartir datos de pacientes clínicos (Qiu et al., 2020). Sea cual sea el aspecto al que se le deba prestar atención, nos plantea el tercer desafío cuya finalidad es determinar el conjunto de herramientas que se van a centrar en "escuchar" los signos vitales para llevar a cabo la diagnosis. Con el conjunto de herramientas nos referimos tanto a componentes hardware como software adecuado. Aunque se destaca la importancia del hardware por la importancia del tamaño, incluimos también el software

porque va de la mano.

3.1.4. Sistema de alimentación del CPS.

Aun con la decisión pendiente sobre el componente físico y el hardware adecuado, la siguiente idea que se plantea es sobre las posibles compatibilidades entre estos elementos a la hora de conectarlos entre sí y a la corriente eléctrica. Es decir, una vez que las herramientas sean elegidas debemos comprobar que varios dispositivos necesiten el mismo puerto a una hipotética unidad de control o que se requieran más enchufes de los que hayan disponibles. Siendo este problema relativamente fácil de subsanar nos traslada al consumo eléctrico que pueda emplear el CPS. A diferencia del consumo que pueda producir un CPS en una cadena de montaje industrial, debemos asegurarnos que nuestro sistema, aunque se encuentre en un entorno casero, no lleve a un consumo excesivo de electricidad. Así que los métodos de ahorro energético deben ser planteados para tal fin, a priori enchufes inteligentes o sistemas de reposo adaptativos a la rutina deben ser tenidos en cuenta al igual que enfoques que brinde la literatura. Algunas alternativas interesantes para examinar son las que propone Ahmed et al. (2015) y Thongkhao y Pora (2016) en las que las características principales de estas propuestas son: bajo coste, bajo consumo, registro de consumo, monitoreo de consumo eléctrico e incluso interfaz web para conectar o desconectar electrodomésticos a distancia. Propuestas como la de Torres-Sanz et al. (2018) se centran en estrategias de carga eléctrica para coches eléctricos y aunque no estemos hablando del mismo sector, su trabajo destaca elementos que a priori pueden ser tomados en cuenta para cualquier modelo eléctrico. Estos elementos son el coste de la electricidad por país, horarios en los que el coste por vatio (W) es más económico o la frecuencia de uso del sistema por parte del usuario, en el caso del artículo el coche.

Independientemente del elemento físico que se use para el CPS, o sin saber que herramientas serán usadas para la parametrización, la manera de alimentar energéticamente al sistema es un factor a tener en cuenta, principalmente por proveer la cantidad de energía adecuada a la cantidad de componentes necesarios. Dado que se trata de un CPS para usuarios comunes y corrientes que no deben de llevar a cabo operaciones especializadas, sino más bien rutinarias, a priori el gasto no debería ser un gran problema. En el caso de que el gasto energético esté dentro de unos límites asumibles, nos hace inclinarnos por el concepto que permita este consumo. Sin embargo, esto da pie a que otras ideas que plantean el mismo fin sean también tenidas en cuenta. Las nuevas ideas estarán centradas en un consumo eficiente de energía más que en reducir la cantidad suficiente de energía. Estas ideas, a priori, pasan en brindar el mismo rendimiento pero de una manera alternativa, como la instalación de sistemas de energías renovables. Otra idea

consiste en modelos de ahorro basados en tecnologías verdes. En estos modelos se efectúa un consumo corriente de energía en función de la rutina del usuario, de manera que exista una funcionalidad de bajo consumo cuando el sistema estime que no requiere vigilar de manera constante al usuario. Así que el tercer desafío de esta tesis es determinar qué método o mecanismo de ahorro de energía o reducción de consumo eléctrico es el más adecuado para este tipo de CPS.

3.1.5. Medidas de seguridad.

El último aspecto que tiene en cuenta la propuesta actual para lograr su principal cometido incide en las medidas de seguridad del CPS. A diferencia de otros sistemas de monitorización, esta estará en un entorno casero e interior en el que a priori estará seguro de golpes, caídas y "manos indecentes" que puedan afectar al correcto funcionamiento, por lo tanto el CPS necesitará seguridad a otros niveles. Dado que en un primer escenario el CPS está a salvo de los daños físicos, la ciberseguridad es el campo que recibirá más prioridad. El trabajo de Khattak et al. (2019) centra sus esfuerzos en detallar y explicar la arquitectura de un dispositivos IoT con diferentes componentes en la capa de percepción. Los autores se centran en los RFID y las redes de sensores inalámbricas (WSN) ya que son los principales componentes de los dispositivos IoT, basado en las predicciones del MIT el cual apunta que "Los RFID son una de las grandes aperturas en tecnologías de la información, que cambiará el mundo." (Jia et al., 2012). Debido a la función de transmisión de información monitoreada y rastreada a nodos receptores o a un centro de control por parte de las WSN, se consideran que son un puente fundamental en el mundo cibernético y el mundo real (Wu et al., 2011). Los ataques a estos componentes están clasificados según la parte del sistema que es afectada. La tabla 3.1 resume los ataques relaciones con los RFID y la tabla 3.2 resume todos los ataques relacionados con las WSN y los ataques de denegación de servicios, ya que según los autores es el ataque más frecuente y común que afectan a sistemas como el actualmente presentado. Estos ataques no se centran en modificar o robar información de los sistemas, si no que tiene como objetivo la disponibilidad y deshabilitación de un sistema ya que pueden enviar o transmitir una gran cantidad de señales para interrumpir o bloquear cualquier nodo o sensor del sistema (Kasinathan et al., 2013).

El trabajo de Khattak et al. (2019) enseña la totalidad de ataques que pueden afectar a un CPS. Sin embargo, dada la variada lista de amenazas presentadas la labor de abordar todas y cada una de ellas puede llevar una cantidad de trabajo desmesurada que a la larga no es objeto de estudio de esta tesis. Así que se cierne la incertidumbre sobre cuál de todas ellas trabajar. Un elemento que genera aún más incertidumbre es saber sobre que se va a basar la elección sobre un sistema cuyas pruebas son recientes y no ha sido

Capa Afectada	Tipo de ataque
Ataques a múltiples capas	<ol style="list-style-type: none"> 1. Ataque criptográfico 2. Ataques por canales laterales 3. Ataques por denegación de servicios 4. Ataques por repetición. 5. Ataques físicos. 6. Ataques por análisis de tráfico. 7. Ataques por desactivación.
Ataques a la capa estratégica	<ol style="list-style-type: none"> 1. Ataques de ingeniería social. 2. Ataques de privacidad. 3. Ataques dirigidos. 4. Ataque de espionaje competitivo.
Ataques a la capa de aplicación	<ol style="list-style-type: none"> 1. Lecturas de etiquetas no autorizadas. 2. Ataque de modificación de etiquetas. 3. Ataques directamente al software.
Ataques a la capa de red	<ol style="list-style-type: none"> 1. Ataque de clonación. 2. Ataque por espionaje o “escucha oculta”. 3. Ataque de suplantación o “spoofing”. 4. Ataque a las redes de comunicación. 5. Ataque de “Man in the middle”.
Ataque a la capa física	<ol style="list-style-type: none"> 1. Remover la etiqueta del RFID. 2. Destrucción de la etiqueta del RFID. 3. Ataque mediante el comando kill. 4. Ataques de interferencia de cualquier señal. 5. Ataque de interfaz pasiva.

Tabla 3.1: Clasificación taxonómica de los ataques a los RFID

desplegado aún al servicio público. Básicamente si el sistema aún no ha madurado lo suficiente es difícil saber cuál es su principal vulnerabilidad, por lo que la elección sobre la seguridad se ve disipada. Aunque la elección no está clara, en materia de seguridad la anticipación es un factor clave por lo que el último obstáculo a abordar en esta tesis es establecer qué aportes en materia de seguridad generan valor al CPS propuesto.

Capa Afectada	Tipo de ataque
Ataques a la capa de transporte	<ol style="list-style-type: none"> 1. Ataque de desincronización. 2. Ataque de inundación.
Ataques a la capa física	<ol style="list-style-type: none"> 1. Ataque de interferencia. 2. Ataque de manipulación.
Ataques a la capa de red	<ol style="list-style-type: none"> 1. Ataque de información de enrutamiento falsificado. 2. Ataque de reenvío selectivo. 3. Ataque Sybil. 4. Ataque por sumidero (Sinkhole). 5. Ataque de agujero de gusano. 6. Ataque de agujero negro. 7. Ataque de agujero gris. 8. Ataque por inundación de "hola". 9. Ataque por suplantación de identidad. 10. Ataque de carrusel. 11. Ataque de estiramiento. 12. Ataque de medusas (Jellyfish). 13. Ataque de vampiro.
Ataques a la capa de enlace	<ol style="list-style-type: none"> 1. Ataque por colisión. 2. Ataque por agotamiento. 3. Ataques injustos.

Tabla 3.2: Categorización y clasificación taxonómica de los ataques DoS en WSNs

3.2. Discusión

Partiendo de las consideraciones anteriores podemos resumir que el propósito del trabajo de esta tesis es presentar un CPS capaz de medir parámetros de importancia para la salud al coste más bajo posible y de manera que la interacción con este sea natural, fluida y prescindiendo de dispositivos vestibles para la monitorización del usuario. La presente sección tratará sobre el análisis llevado a cabo para la toma de decisiones de varios aspectos sobre el enfoque propuesto.

La propuesta actual se ha ido formando gracias a la superación de los distintos desafíos planteados en los epígrafes anteriores y el cual está soportado por todo el capítulo 4. En cuanto al soporte físico, se ha recurrido a una revisión de la literatura para poder determinar cuales son los soportes físicos más usados en el ámbito del cuidado de la salud y los CPS, además de indicar que elementos monitorizan o que utilidad adicional aportan. Teniendo en cuenta los resultados de la revisión de la literatura destacamos las sillas, ya que se han usado para analizar la actividad del usuario mediante sensores como lo muestra el trabajo de Bassoli et al. (2018), o para determinar la ocupación del espacio útil en una oficina (Labeodan et al., 2016). Pese a que no es un proyecto del ámbito del cuidado de la salud sí que cumple los requisitos para pertenecer a la categoría de CPS ya que la detección del espacio útil se hace con el fin de mejorar el consumo energético en una planta de oficina. El análisis del uso del espacio se lleva a cabo con técnicas de medición de vibración y tensión, para ello se han instalado sensores en los respaldos. Otro soporte físico usado para monitorizar al usuario son las camas, para este caso vemos como el trabajo de Spillman Jr et al. (2004) en el que proponen una cama como método no invasivo para monitorizar la respiración, frecuencia cardiaca y movimientos del paciente. Otros trabajos como el de Yousefi et al. (2011) tratan patologías más específicas y más caras en términos médicos y de recursos humanos como las úlceras por presión. La siguiente propuesta de componente físico es un armario que ha sido usado para reconocimientos de actividad (Whitehouse et al., 2018) a través de sensores instalados en los compartimentos o para el seguimiento de artículos que deban ir en determinados compartimentos (Ramírez et al., 2019). Como soporte final, tenemos las mesas, las cuales han sido usadas para la educación primaria de niños con la función de identificar varios objetos que hayan sido situados en la superficie (Steurer y Srivastava, 2003) o para centrarse en temas más específicos como la nutrición alimenticia y las costumbres alimenticias mediante sensores de presión que pueden detectar el peso y maneras de comer, como beber bebidas, cortar y pinchar alguna pieza de comida (Zhou et al., 2015).

La decisión final fue un armario de cocina. Esta decisión estuvo basada en

	Silla	Cama	Armario	Mesa
Facilidad de uso	Si	Si	Si	Si
Forma homogénea	No	Si	No	No
Posibilidad de daño	No	Si	Si	No
Compartimentos	No	No	Si	No
Posibilidad de conexión a la red eléctrica	Si	Si	Si	No
Parametrización	Peso, Temperatura, Postura, Frecuencia cardiaca	Peso, Altura, Temperatura, Postura, Sueño.	Memoria, Información nutricional, Información alimenticia.	Ninguno relevante.

Tabla 3.3: Criterios de selección del componente físico

las prestaciones y criterios que satisfacen este soporte en comparación de sus iguales. Además, bajo nuestro punto de vista es el elemento físico que más se ajusta a nuestra investigación sobre diagnóstico. Los criterios de selección del soporte físico están resumidos en la tabla 3.3.

Tal como se ve en la tabla 3.3 los criterios de selección fueron facilidad de uso, forma homogénea, posibilidad de daño, cantidad de compartimentos, posibilidad de conexión a la red eléctrica y tipos de elementos que se pueden parametrizar. La facilidad de uso se refiere a la ausencia de un medio o a la realización de un proceso por parte del usuario para aprender a usar ese componente físico. Dado que los candidatos son muebles que un usuario común puede tener en su hogar o puede haber usado muchas veces a lo largo de su vida, no tiene que aprender a usarlos, por lo que todos los candidatos en este campo son muebles potenciales a ser usado como componente físico. Además tratando de homogeneizar la selección, se pueden encontrar modelos de sillas tan dispares donde ubicar sensores, por ejemplo en el caso de Bassoli et al. (2018) encontramos que el modelo de la silla usado permite poner los sensores en el espaldar de la silla y en el caso de He et al. (2018) los sensores están en el asiento. En cuanto al armario y la mesa, la gran cantidad de armarios y mesas disponibles en el mercado es amplia por lo que podemos encontrarnos con formas cuadradas, rectangulares, y a diferentes alturas, por lo que es mejor centrarse en un armario o mesa para una tarea específica, como por ejemplo un armario de cocina o una mesa de noche.

Debido a esta razón y a falta de examinar más criterios se mantienen fuera del soporte ideal. En el caso de las camas, no hay tanta variedad más allá de literas, aun así la cama seguiría manteniendo una forma homogénea por lo que se mantiene como candidata ideal.

Dado que el soporte físico va a albergar componentes electrónicos, hardware y previsiblemente cables, este soporte debe garantizar o por lo menos reducir al máximo la posibilidad de daño que puedan sufrir estos componentes, ya sea por accidente, como por ejemplo que el usuario mueva el soporte hacia algún lado y los componentes vuelquen. En este caso conservamos la cama y el armario debido a que son elementos que el usuario a priori no debería mover en su casa con mucha frecuencia, dado a que estos pesen mucho o simplemente ocupan un gran espacio en casa y no se puedan ser desplazados tan fácilmente en comparación con otros como la mesa y la silla. Aparte de esto, las posibilidades para almacenar sistemas electrónicos son altas, ya que estos elementos pueden contener compartimentos o sitios donde pueden hacer reposar el hardware. El trabajo de Zhou et al. (2015) consiste de una mesa inteligente para el monitoreo de la nutrición. El dispositivo que usa para realizar tal monitorización es una tela equipada con una matriz textil fina y una tableta sensible al peso, sin embargo esta tela no ocupa toda la mesa y todos los componentes que cubre son sensibles al derrame de líquidos. Este tipo de configuración no implica ningún tipo de seguridad para el mecanismo o soporte físico, por lo que nuestra propuesta es reticente al uso de este tipo de tecnología, así que debemos despreciarla. Por lo tanto la mesa queda descartada en este ámbito.

En cuanto a la silla, la revisión indica que todos los proyectos de monitorización de la salud e IoT incluyen sus sensores y cableados en el interior de los cojines de la silla, en el respaldo o en ambos como en (Ahn et al., 2015) de tal manera que estos sitios ofrecen un lugar seguro para el hardware. Sin embargo esto limita mucho la elección del soporte físico ya que requiere unas características específicas, como modelos concretos de sillas que no todos los usuarios pueden tener, o incluir una caja protectora anexada al reposabrazo para almacenar el hardware, que hace la función de envoltorio protector como se muestra en (Ganesh et al., 2016). Dadas las condiciones exclusivas de esta característica descartamos la silla también.

La sección de compartimento se ha tenido en cuenta principalmente porque ofrece, a priori, sitios donde guardar el sistema, hardware, cables etc, y porque ofrece interacción indirecta con el usuario que posteriormente puede dar juego a parametrizar aspectos de la conducta del individuo como lo demuestra el trabajo de Whitehouse et al. (2018). Este trabajo realizó un estudio de la conducta con ayuda de sensores situados en las puertas de los compartimentos de un armario, por esa razón mantenemos el armario como

opción viable para este caso, aunque siendo precavidos en el mecanismo de estos compartimentos por si puede llegar a ser un factor clave o de importancia. Es decir, dada la variedad de armarios con compartimentos, no todos estos se han de abrir de la misma manera, algunos de ellos pueden ser abatibles, abrirse de izquierda a derecha, de arriba hacia abajo, entre otros. Así que veremos si estos mecanismos de apertura influyen de alguna manera en el proceso de diagnóstico. La mesa y la cama quedan descartadas, ya que no todas las mesas y camas poseen compartimentos y en el caso de las camas, su frecuencia de uso no es alta ya que estaríamos hablando de camas con canapés o con un solo compartimento. Algunas sillas o sillones no poseen un compartimento al uso, sino más bien bolsas o huecos donde se pueden almacenar cosas, como mandos a distancias o revistas.

En el apartado final, el de parametrización, se ha tenido en cuenta el tipo y la cantidad de parámetros que se pueden medir a priori con ayuda de los muebles candidatos. Este apartado puede sonar el más subjetivo o incluso el que menos utilidad puede aportar, ya que previamente se ha manifestado como objetivo el estudio de la memoria, sin embargo se deben establecer qué parámetros son necesarios para tal fin, algo que no ha sido previamente definido. En esta categoría la mesa queda completamente descartada, ya que sus formas variopintas no permiten medir un patrón en concreto y si tenemos en cuenta que en una mesa no necesariamente se ha de apoyar un solo usuario ya implica un dispositivo de rastreo en los usuarios para determinar cuál de ellos está teniendo contacto con la mesa o con los objetos que están sobre esta, esto no es lo deseado ya que queremos librar al usuario de cualquier wearable.

Aparte de esto las mesas son muebles en los que normalmente no sólo se apoya el usuario, si no que también reposan objetos ya sea por decisión o por omisión del usuario y puede afectar al presente estudio. La silla, la cama y el armario, poseen un mismo inconveniente que pueden ser usados para cuyo fin no ha sido construido y puedan entorpecer la obtención de datos u obtener datos erróneos. Es decir, estos elementos pueden ser utilizados para hacer reposar objetos, o incluso en el caso de la silla puede ser usada a modo de escalón para alcanzar algún objeto a una determinada altura. No obstante, y de manera subjetiva, si tenemos en cuenta la superficie de una silla esta no es tan basta como para reposar tantos objetos; las camas contienen almohadas, sábanas, mantas, objetos que no son propiamente ajenos al entorno donde se encuentran y pueden ser tenidos en cuenta en un posible error de muestreo que se obtenga. De la misma manera sucede con los armarios, a manera de resumen es bastante infrecuente encontrarse en un armario de ropa vasos, platos, cubiertos o viceversa, e incluso en el mejor de los casos el contenido no resulta relevante para nuestro cometido. Dado que estas situaciones pueden darse una cantidad escasa de veces mantenemos estos tres últimos como elementos viables. Por lo tanto, la silla, la cama y el armario

son los soportes más idóneos ya que no poseen las desventajas de la mesa, son muebles que aportan comodidad al usuario, y en el caso de la cama y la silla su uso no puede variar de muchas maneras.

Todas estas líneas debatiendo sobre los rasgos y pormenores de la elección del componente físico, es por que lo consideramos de gran importancia para nuestra propuesta ya que en cierta medida condiciona al resto de componentes. El ejemplo más notable es la interacción que va a tener el usuario con ese componente y para que esa interacción sea posible es determinante ubicar los nodos pertenecientes a la capa de percepción en el sitio adecuado. En la sección 3.1.2 establecimos el debate sobre las maneras de interactuar más adecuadas. Uno de los puntos de ese debate era sopesar las opciones que teníamos para poner en marcha el sistema o hacer que el usuario ponga en marcha el sistema mediante su intervención. La solución más viable pasa por una mezcla de ambas propuestas. Dado que queremos dar más importancia a las interfaces invisibles el elemento por naturaleza que más se ajusta a nuestra propuesta son los sensores, por ello serán los elegidos para ser implantados en el sistema, al menos en una etapa temprana. Sin embargo no queremos desechar tan prontamente los RFID principalmente para aprovecharlos en el futuro, y es que dada la gran prestación de servicios que pueden ofrecer los CPS como se ve en las figuras 2.1 y 2.2 es posible que su uso sea necesario para expandir servicios o aumentar prestaciones.

Siguiendo con lo planteado en la sección 3.1.2, el otro tema relacionado con la interacción era otro mecanismo usado potencialmente para la configuración del CPS. Este nuevo mecanismo debe tener en cuenta los aspectos necesarios para que el usuario, y no necesariamente el usuario objetivo, pueda llevar a cabo la configuración, e incluso el montaje del sistema en el hogar. Sin embargo, el principal impedimento es determinar qué va a ser medido y mediante qué componentes, de esta manera puede ser acotada esta manera de interactuar. No obstante, dado que la intención es usar sensores o una red de estos, las señales que capturan estos sensores deben ser interpretadas y traducidas por alguna unidad central a la que estén conectados estos sensores y además, que permita establecer comunicación con ella. Por lo tanto, una vez que la unidad de control sea establecida la manera de comunicarse con el usuario debe estar basada en una solución web, aplicación de escritorio o aplicación móvil. Lógicamente con la unidad determinada y los otros elementos definidos, este método de interacción quedará definido de igual manera. Para zanjar esta cuestión, consideramos que un correspondiente estudio sobre usabilidad y facilidad de uso facilitará la toma de decisiones.

Regresando al tema de la unidad central de control y para proveer de una alternativa al tema planteado en la sección 3.1.3, herramientas de medición, se han valorado placas de ordenadores reducidas de bajo coste como la RP

o Arduino presentadas en la figura 3.1. Ambas placas en aspecto físico son bastante parecidas y ambas coinciden en que pueden ser usadas en muchos proyectos de electrónica. La aparición de ambas placas fue suplir una carencia de aprendizaje en las aulas, concretamente facilitar el uso de la electrónica y la programación a un coste relativamente bajo. A pesar de que las dos se usan para proyectos comunes, son dos conceptos diferentes, lo que complica un poco su comparación. Una de las principales diferencias es la filosofía del hardware, en el caso de Arduino es abierto para que cualquiera pueda crear versiones personalizadas de la placa, esto es algo muy positivo ya que si nuestro sistema demanda alguna personalización en particular estamos en posición de satisfacerla. En comparación la Raspberry Foundation tiene el control total sobre sus placas y solo ellos pueden fabricarlas. En otros aspectos, la placa de Arduino tiene como punto fuerte la capacidad de conectarse con un mayor cantidad de dispositivos gracias a sus puertos tanto analógicos como digitales. La RP no posee tanta versatilidad en ese aspecto ya que ha sido diseñado como un pequeño ordenador, pero compensa esa carencia con mayor potencia de cálculo. En cuanto a software también hay diferencias destacables, como por ejemplo que la placa de Arduino ejecuta automáticamente cualquier tarea para la que haya sido programada y dado que la RP ha sido fabricada como un mini ordenador requiere la espera del arranque de su sistema operativo y otros elementos. En este sentido, la RP es más lenta que su análoga lo cual puede incidir directamente en el proyecto, en la forma de configurarlo y en la forma de programarlo tal es el caso que para encender un diodo emisor de luz (LED) en Arduino consta de unas pocas líneas de código, mientras que en la RP hace falta descargar librerías, instalarlas, configurarlas y compilarlas. Como última característica a comparar entre estos dos dispositivos es la conectividad, la RP cuenta con WiFi y puerto Ethernet ya integrado por lo que no sería ningún extra necesario a diferencia de la placa de Arduino. Esta última puede lograr el mismo tipo de conectividad a costa de gastar algún puerto y encarecer un poco más el precio de la placa. Analizando estudios como el de (Ferdoush y Li, 2014) cuyo trabajo se centró en el diseño de una red de sensores para aplicaciones de monitorización ambiental usando una RP y una Arduino, y uno de sus componentes fue un portal web para visualizar y configurar parámetros, es fácil darse cuenta de todas estas comparaciones. La red de sensores fue construida usando estas dos placas de manera conjunta y teniendo en cuenta que los autores alegaron que ambos dispositivos son compatibles la decisión final quedará relegada a detalles de muy poca importancia o que marquen relevancia en el estado que se encuentra el CPS.

En el hogar prácticamente todos los equipos y electrodomésticos funcionan con energía eléctrica, pero no todos realizan el mismo consumo. El gasto energético depende de varios factores como: tiempo de servicio, potencia no-

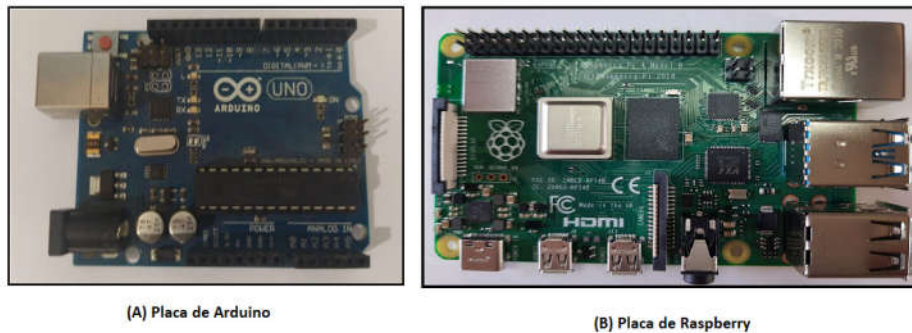


Figura 3.1: Placas de procesamiento

minimal, necesidad de uso por parte del usuario, entre otros. Esto nos conduce a plantear las reglas para mecanismos de ahorro.

Antes de discurrir sobre qué mecanismo de ahorro es el más adecuado, es conveniente aclarar cuál es el consumo teórico actual y si realmente merece la pena invertir esfuerzos en este aspecto, para ello estimaremos el consumo teórico de una placa como la RP. La estimación es efectuada calculando la potencia de la placa, la ecuación 3.1 presenta como es el cálculo de esta.

$$Vatio(W) = Amperio(A) \cdot Voltio(V) \quad (3.1)$$

Según la ecuación 3.1 la unidad de potencia usada es el Vatio (W) y su definición es la tasa a la que circula la electricidad cuando una corriente de un Amperio (A) fluye a través de una diferencia potencial de un Voltio (V). Según la documentación oficial de RP (<https://www.raspberrypi.org/documentation/faqs/>) el adaptador oficial de corriente funciona a 5 V y provee de una intensidad máxima de 3 A, resultando así 15W teóricos. La documentación oficial también indica que aunque el adaptador de corriente tenga una intensidad máxima de 3 A, no quiere decir que esta sea toda la corriente que esté usando en todo momento. De hecho se distingue el consumo por escenarios, los cuales son: en reposo, reproduciendo vídeo y en máximo estrés. Si tomamos como ejemplo uno de los modelos más recientes de placa como la RP 3B+ la intensidad para el reposo es de 0.3A, 0.55A para la reproducción de vídeos y de hasta 1.34A en estrés máximo, si aplicamos la ecuación 3.1 obtenemos como resultado: 1.5W, 2.75W y 6.7W para reposo, vídeo y estrés máximo respectivamente.

Hasta aquí se determina que el consumo mínimo y máximo de una RP oscila entre 1.5W y 6.7W, sin embargo estos datos no aportan luz al tema sin ser traducidos monetariamente. Para saber cuando le supone al usuario el

simple consumo de la RP hace falta fijarse en el cobro que está ejerciendo la compañía eléctrica por el kilovatio hora (kWh) y si aplica algún tipo de descuento por franja horaria. Ahora estimaremos el consumo teórico máximo y mínimo a lo largo de un año, por tanto:

$$1.5 W \cdot 24 \text{ horas} = 36 W \text{ al día}$$

$$36 W \cdot 365 \text{ días} = 13,140 W \text{ al año} = 13 \text{ kWh al año}$$

$$6.7 W \cdot 24 \text{ horas} = 160.8 W \text{ al día}$$

$$160.8 W \cdot 365 \text{ días} = 58,692 W \text{ al año} = 58 \text{ kWh al año}$$

Una vez la potencia anual es calculada, ya solo es necesario saber el precio del kWh, el cual viene anexado en la factura de la luz, para este supuesto tomaremos como coste 0.13 euro por kWh, con lo que obtenemos:

$$\text{Coste en reposo: } 13 \text{ kWh} \cdot 0.13 \text{ euro/kWh} = 1.69 \text{ euro}$$

$$\text{Coste en estrés máximo: } 58 \text{ kWh} \cdot 0.13 \text{ euro/kWh} = 7.54 \text{ euro}$$

Siempre se ha hablado de consumo teórico, por que depende de más factores estimar el consumo exacto, incluso periféricos que estén conectados a la RP como teclados o ratones hacen que el gasto aumente. No obstante con esta estimación el lector podrá hacerse una idea de la magnitud del gasto aproximado del CPS en un año. Relativamente, no es un gasto exagerado, pero en términos absolutos la comparación del consumo en reposo y en estrés máximo hay una gran diferencia, tanto así que el dispositivo en total reposo supone un ahorro del 77.58%. Lógicamente esta cifra no es alcanzable ya que el CPS no siempre, y por consiguiente la placa de procesamiento, no estará en reposo total, así que la mejor solución para afrontar el entresijo de la sección 3.1.4 pasaría por distinguir aquellos momentos en los que el sistemas pueda estar en reposo sin que suponga una pérdida de información para la diagnosis.

Para culminar con esta sección se afronta la solución al tema de la seguridad en el CPS. Este tema es especialmente complejo de afrontar debido a la ausencia de experiencia de trabajar con sistemas de tales características, por lo que solo está disponible lo que la literatura puede ofrecer. Además de esto el sistema se encuentra en una etapa primeriza y no ha sido expuesto a ninguna amenaza, por lo que no hay un objetivo potencial sobre el que defenderse. No obstante el trabajo de Khattak et al. (2019) ofrece un listado completo sobre los principales ataques a sistemas de esta índole. Este listado de ataques están basados en ataques DoS que tienen como objetivo comprometer al sistema. Volviendo al tema de la falta de foco en un ataque en particular, y planteando una solución al debate discurrido en la sección 3.1.5 se propone de una herramienta de análisis y anticipación. Así que esta herramienta será un simulador que permita definir comportamientos de

ataques DDoS. Mediante la simulación se puede ofrecer una herramienta no solo para el beneficio propio del CPS, si no que también pueda extenderse a otros ámbitos. Además de la misma medida que se pueden simular ataques se pueden obtener contraindicaciones para poder actuar de la forma más rápida e inmediata ante la caída del sistema.

Finalmente, con una visión más objetiva y clara sobre cómo abordar detalles acerca del diseño de un CPS en el ámbito de la salud realizada en esta sección, concluimos con el enfoque definitivo. La sección 3.3 presenta al detalle el CPS diseñado que se ha denominado como Armario Inteligente y cuales han sido los componentes elegidos para formarlo.

3.3. Planteamiento del trabajo: Armario inteligente.

Una vez la comparación de los soportes físicos se ha llevado a cabo parece fácil darse cuenta que la opción natural del soporte no pasa por la silla o la mesa, ya que en la tabla 3.3 presentan el menor número de ítems positivos y tienen menos aspectos parametrizables o más irrelevantes.

A partir de aquí, las dudas promueven un debate entre el armario y la cama. En el caso de una cama, como parámetro a monitorear tenemos el sueño y para ello necesitamos un registro polisomnográfico, el cual consiste en el registro simultáneo del electroencefalograma, el electrooculograma, el electromiograma de los músculos submentonianos, el electrocardiograma y la respiración (Peraíta-Adrados, 2005) o lo que es lo mismo un registro de la actividad cerebral, de la respiración, del ritmo cardíaco, de la actividad muscular y de los niveles de oxígeno en la sangre mientras se duerme. Si el usuario presenta algún tipo de trastorno se puede monitorizar temperatura rectal, tensión arterial, movimiento de las extremidades, gases sanguíneos, presión endoesofágica, erección peneana y reacción electrodérmica (Rechtschaffen, 1968), (Billiard, 2003). Otro parámetro a controlar es el índice de masa corporal que podemos obtener a partir de la estatura y el peso, y con el cual podemos indicar al usuario problemas derivados de la obesidad (Prentice y Jebb, 2001) o incluso con la diabetes (Bays et al., 2007). Como parámetro final para parametrizar con una cama como soporte físico para un CPS es la postura corporal de manera que se pudiese informar al usuario de malformaciones o lesiones derivadas de una mala postura.

Sin embargo tanto la polisomnografía como el estudio postural implican grandes inconvenientes que pueden incurrir en elevados costes y más importante aún limitan la libertad de movimiento del paciente. En cuanto al registro polisomnográfico, dada la cantidad de datos que se obtienen mediante el,

construir un CPS para tal soporte sale de los rangos de dispositivos “low-cost” que un usuario podría permitirse y que podríamos construir. Un CPS de tales características, implican ventosas, electrodos, electrocardiográficos y otros elementos que las clínicas y hospitales pueden permitirse. En el caso de que tal CPS pudiese construirse dentro de los parámetros del “low-cost”, para realizar el registro polisomnográfico debemos modificar algunos hábitos del paciente ya que este estudio implica que el usuario no tome estimulantes como por ejemplo té, café, coca-cola, alcohol, no tome siestas y evite fármacos que puedan afectar al sueño.

Finalmente, un estudio de esta índole implica un entorno cableado con ventosas que no es agradable o al menos cómodo para el usuario y su amplitud de movimientos.

El siguiente parámetro a tener en cuenta es un estudio postural, trabajos como el de García-Magariño et al. (2017) aportan las primeras “pinceladas” sobre cómo empezar a abordar este tema, proponen un sistema de simulación basado en agentes para camas inteligentes. En este proyecto los autores realizan la simulación de una cama inteligente como una red de sensores de carga situados en forma de cuadrícula, de manera que mediante el simulador pueden ejercer presión sobre uno de los sensores para representar zonas del cuerpo. A pesar de que no indican cómo puede ser usada la información que se extrae, el sistema provee información valiosa del cuerpo cuando este está girado hacia un lado, o está en una posición frontal, cuando el cuello está doblado, o cual es la posición de la espina dorsal y el tiempo que se está en una determinada posición. Sin embargo, a pesar de que el simulador arrojó resultados muy buenos y prometedores los autores señalan que trasladar el simulador a una matriz de sensores físicos reales incurre en altos costes que sobrepasan el concepto de low-cost. La alta cantidad de sensores se debe a que son necesarios para obtener de manera muy precisa las posiciones del cuerpo. Entre otros inconvenientes menores añadimos que un proceso de calibración es requerido para usar la matriz de sensores, por lo que añadiríamos un escenario más al usuario para el uso de esta tecnología de lo que se desprende un proceso cognitivo adicional. Otros tipos de cama para el estudio de la postura conllevan modelos de camas más engorrosas o modelos no convencionales que no hay en todos los hogares (Dixon et al., 2001).

En cuanto al índice de masa corporal, parece la opción más idónea ya que con situar mecanismos para el peso y la estatura sería suficiente para tener un CPS semi funcional, sin embargo algunos elementos fueron obviados que hicieron que esta no fuese la opción más clara para un soporte físico. No había ninguna garantía que los usuarios tuviesen una cama individual o compartida, aparte de esto si la cama es compartida el peso del acompañante estaría influyendo en nuestros cálculos. Tampoco se ha tenido en cuenta

objetos variables que puedan estar en una cama, como almohadas, colchas, peluches o mascotas.

La contraparte de la cama es el armario, en el cual desechamos todos los parámetros anteriormente mencionados y optamos por unos nuevos como la memoria y la información nutricional. Sin embargo, la manera y los mecanismos necesarios no han sido definidos para tal fin. Para realizar un correcto seguimiento nutricional de los alimentos ingeridos por el usuario, es necesario el inventario de los productos alimenticios y determinar un seguimiento de alimentos por compartimentos. Los elementos más frecuentes para realizar tal fin requieren al menos de un lector de código de barras y sensores que detecten las aperturas de las puertas, pero aun así la información nutricional no estaría completa ya que alimentos como frutas, pan, patatas suelen carecer de códigos de barra que pueda identificarlos, para solventar tal inconveniente podemos añadir una cámara y con la ayuda de algoritmos de reconocimiento de imágenes con Opencv podemos realizar una aproximada estimación de su volumen (Hassannejad et al., 2017). Sin embargo este enfoque tiene cabos sueltos como proporcionar toda la información de los alimentos que se almacenen en el armario, la incertidumbre de saber la cantidad exacta que consume cada usuario, es bastante normal tener un paquete de harina en la cocina o una bolsa de arroz y no usarla toda, sino guardar el restante por lo que es necesario llevar un seguimiento del peso de cada alimento lo cual implica que los inconvenientes progresen de manera geométrica.

El seguimiento realizado por el usuario del peso de cada alimento es inviable, ya que aunque la tarea no sea ardua mediante una interfaz de voz o aplicación, puede que no resulte agradable si al momento de seguir una receta ha de estar constantemente cambiando pesos y siguiendo pasos, además que esto puede implicar un pequeño descuido y no realizar el seguimiento correctamente, así que debido a esta razón el CPS prescinde del estudio nutricional o alimentario.

Una de las principales ventajas de un estudio nutricional incide en la obesidad, ansiedad y otros problemas derivados, por ejemplo el trabajo de Oddy et al. (2009) informa que una de las razones en la mala conducta en los adolescentes viene de la ingesta de comida chatarra, caramelos y malos hábitos de alimentación. Otra de las ventajas que se puede extraer de un estudio nutricional es prevenir al usuario sobre la gestión de su estrés. Cuando una persona ha pasado un día muy estresante o ha pasado por situaciones que le han conllevado un gasto adicional de energía, su cuerpo tenderá a segregar más insulina para compensar el gasto energético hecho, por lo tanto muchas veces se recurren a determinadas fuentes de insulina. Algunas de estas fuentes de insulina pasan por la ingesta de comidas en alto contenido de grasas y colesterol, y el principal problema de estas es que promueven la

obesidad (Farzi et al., 2019). Esta situación es altamente peligrosa, porque se ha demostrado que el vínculo entre emociones y alimentación en personas que sufren obesidad es mucho más fuerte que en las que no (Sánchez Benito y Pontes Torrado, 2012), por lo que da a entender que estados de ánimos negativos tienen una alta influencia en la aparición de trastornos alimenticios (Cooper y Taylor, 1988). Siguiendo la línea de lo comentado se ha demostrado que los comportamientos relacionados con desórdenes alimenticios, han sido parcialmente explicados por la presencia de síntomas de ansiedad y depresión (Calderon et al., 2010), por lo que es evidentemente apreciable la relación que hay entre todos estos términos, tal dado el caso que se ha sugerido que en las campañas de prevención de la obesidad se deba incluir la ansiedad como síntoma a evaluar (Goossens et al., 2009), (Courtney et al., 2008)).

A diferencia de la cama, un elemento como el armario al disponer de compartimentos permite el estudio de la memoria mediante patrones del usuario. Con el estudio de la memoria podemos informar al usuario posibles indicios de sufrir enfermedades neurodegenerativas como el Alzheimer. Según el trabajo de Rentz et al. (2011) se han encontrado grandes cantidades de beta amiloide en los cerebros de pacientes que sufren o han sufrido la enfermedad de Alzheimer, sin embargo esta no es una condición sine qua non.

En primer lugar la amiloide es una proteína que se encuentra en el organismo y juega un cierto papel en la función cerebral. En el cerebro de una persona con Alzheimer las proteínas amiloides se acumulan y agregan, estos cúmulos se denominan placas. Las placas de amiloides son una característica importante de la enfermedad (Lahiri y Maloney, 2010). La comunidad científica aún está trabajando duro para determinar cómo este factor de riesgo juega un rol en el transcurso o desarrollo de la enfermedad. El tipo de amiloide que se asocia con la enfermedad del Alzheimer es la beta amiloide (Lahiri y Maloney, 2010). Los niveles de beta amiloide se pueden medir en el líquido cefalorraquídeo o por medio de una tomografía de emisión de positrones cerebral (Fagan et al., 2006), (Johnson, 2006), (Mintun et al., 2006). Se cree que estas placas de beta amiloide son un signo precoz de daño en las células nerviosas, pero aún se está investigando.

Las placas pueden empezar a crearse entre 20 y 30 años antes de que aparezcan los síntomas, pero aún no se sabe a ciencia cierta cómo aparecen estos síntomas y cómo finalmente causan demencia asociada al Alzheimer. Es destacable saber que muchas personas entre 80 y 90 años con placas de beta amiloide en el cerebro no presentan síntomas de demencia, por lo que tener niveles anormales de proteína beta amiloide conlleva el riesgo de desarrollar demencia en un futuro, pero no es una certeza absoluta.

Los niveles de amiloides son uno de los muchos factores potenciales que pueden determinar el riesgo de una persona de desarrollar demencia asociada al Alzheimer. Además, los niveles de amiloides pueden variar a lo largo del tiempo. No todas las personas con valores anormales de beta amiloide desarrollarán demencia, una comparación más familiar o más cercana podría ser el caso de que no todas las personas con tensión arterial elevada desarrollan enfermedades cardiovasculares o sufren un ictus.

De vuelta al trabajo de Rentz et al. (2011), lograron evidenciar la relación entre un exigente examen de memoria, en el que asocian pares de caras y nombres, la beta amiloide y el deterioro de la memoria en sujetos cognitivamente normales, determinando altos niveles de beta amiloide en sujetos con más fallos en el test. Por otro lado el trabajo de (Becker et al., 2009) y el de (Ishii et al., 2016) evidenciaron el estudio y estimación de enfermedades neurodegenerativas a través de patrones del comportamiento y dispositivos IoT, como un cajón inteligente, concluyendo en la posibilidad de conseguirlo mediante elementos como RFID. Dada esta circunstancia, si un armario al que se le instala sensores puede otorgar información sobre cuántas veces se abre, en qué momentos del día y durante cuánto tiempo está abierto, es un candidato a convertirse en el componente físico idóneo. Si el cotejamiento de la información obtenida del armario es contrastado con un test de caras y nombres, y este arroja una correlación positiva nos encontraremos frente a una potente herramienta de medición de memoria.

Además, si nos centramos en un armario específico como el que podemos encontrar en una cocina el contenido puede ser filtrado y podemos trabajar con él, para este caso podemos contar con la información alimentaria o nutricional, por todo esto y las virtudes antes mencionadas el armario de cocina es elegido como soporte físico del CPS. Con esta elección se asientan los cimientos sobre las decisiones de diseño, cuyas elecciones estarán basadas en este componente en pro de diseñar un CPS funcional. Además, se establece que el CPS llevará a cabo mediciones de la memoria con el objetivo de informar al usuario de posibles pérdidas de memoria.

Siguiendo con las consideraciones de las secciones anteriores, una de las principales directrices del CPS propuesto es que la interacción por parte del usuario debe ser natural, fluida y nada “pedregosa”. En este punto se plantea cómo un usuario puede interactuar con un armario de cocina sin entorpecer el uso en sí de este. Si la manera más sencilla de usar un armario de cocina es abrir un compartimento, revisar su contenido y tomar algo de adentro esta no ha de ser cambiada o variada a menos que el cambio aporte algo de valor o de utilidad. En este punto es donde destacan las interfaces invisibles, haciendo posible que se pueda interactuar con el CPS sin ningún dispositivo de seguimiento, sino más bien, con elementos propios del compo-

nente físico. Esta interacción es posible gracias a que cada compartimento del armario poseerá sensores para detectar aperturas y cierres, de esta manera se determinará cuando y como un usuario interactúa con el.

Por otro lado, indicamos que había otra manera más de interactuar. Esta constituye una manera más "tradicional" de interactuar y consta de una aplicación. Esta aplicación no tiene que ser usada exclusivamente por el usuario al que va destinado el CPS, sino que puede ser usada por otros miembros de la unidad familiar o cuidadores cercanos. La aplicación proveerá de varios usos, uno de ellos responde a la configuración y establecimiento de prioridades en el sistemas. Este uso permitirá configurar manualmente el algoritmo de adaptación para el ahorro de energía, del que hablaremos más adelante, también permite establecer qué tipo de elemento o servicios deben ser puestos en marcha cuando se inicie el sistema. El otro uso destacable de la aplicación está en su labor explicativa, cuya finalidad principal es la de demostrar cómo debe realizarse la instalación y configuración de un sistema IoT mediante el uso de avatares. Estos avatares indicarán al usuario como debe estar situado cada elemento en el armario y cómo deben efectuarse las instalaciones. Finalmente, esta aplicación da pie a configurar cualquier aspecto más o proveer cualquier utilidad adicional que fuese necesaria si el CPS amplía sus servicios.

Una vez establecido el soporte físico y los mecanismos de interacción, queda definir el elemento que permite relacionar estos dos componentes directamente y que supone el núcleo del sistema, y no es más que otro que la placa de procesamiento. En la sección anterior se ha dilucidado sobre las cualidades de los dos modelos propuestos, RP y Arduino. La decisión definitiva ha sido la RP. Esta decisión estuvo basada en la experiencia de trabajo previa con este dispositivo y el estado actual de producción del CPS. En primer lugar, la previa experiencia de la que se dispone al trabajar reduce la curva y el tiempo de aprendizaje de trabajar con una determinada tecnología. Hasta aquí una elección lógica, pero la importancia de la elección recae en el estado actual del sistema, esto quiere decir que en el estado que se encuentra el desarrollo del CPS basta con una RP modelo 3B+. El armario de cocina se encuentra en un fase de prototipado, por lo que es sensible a cambios y una mayor explotación de sus servicios, pero aún sin saber cuáles serán esos posibles cambios es mejor contar con una placa con mucho potencial en el procesamiento. Por lo tanto, la flexibilidad ante cambios es más amplia y facilita la transición a un CPS mucho más completo sin la necesidad de una inversión monetaria adicional. Por ejemplo, si el trabajo presentado consta de crear un autómatas que deba seguir órdenes predefinidas para realizar un movimiento, con una Arduino sería más que suficiente, pero si ese autómatas necesita interpretar señales del entorno obtenidas mediante sensores y en función de estas señales deba moverse, la RP es la opción indicada. Esto no quiere decir que el modelo 3B+ sea el definitivo, siguiendo la filosofía

low-cost si el sistema pasa a un campo comercial y debe crearse de manera industrial, existen modelos de RP más baratos que la 3B+. No obstante, la conexión de sensores a estos modelos incluyen el soldado en placa, por lo que están más enfocados a un producto final.

En materia eléctrica el CPS no supone un consumo especial, ni ninguno de sus componentes supone un gasto alarmante de electricidad, así que se puede mantener una conexión rutinaria a la corriente eléctrica mediante cualquier enchufe de pared. No obstante somos conscientes que un sistema de estas características no es necesario que esté a pleno rendimiento las 24 horas del día, ya que un usuario tiene sus horas, para descansar, dormir y estar por fuera de casa. Estas horas suponen un gasto innecesario que el CPS no debería efectuar. En un primer momento se optó por enchufes inteligentes, cuyas horas de funcionamiento podrán ser programadas para que el paso de corriente a la RP se efectuase en momentos determinados del día. Esta solución estaba bien a medias, ya que el usuario puede cambiar su rutina sin previo aviso. La solución definitiva a este problema, y a la postre que supone un ahorro en el CPS, fue diseñar un algoritmo que adapta su funcionalidad a la rutina del usuario. Dado que la interacción con el usuario aporta, entre otras cosas, en qué momento del día se interactúa con éste, es viable obtener los rangos horarios en los que más aperturas y cierres se efectúan. Gracias a estos rangos horarios la estimación sobre la rutina del usuario puede ser calculada de manera que el algoritmo “aprenda” cuando debe estar a pleno rendimiento y cuando debe estar en reposo. Teniendo la estimación de los rangos horarios calculada, se produce cierta sensibilidad a la escucha de aperturas y cierres fuera de esos rangos horarios, de manera que si el usuario cambia su rutina, este algoritmo puede desplazar esas horas de pleno rendimiento a otra franja horaria. Al desplazar las franjas horarias el algoritmo se puede ajustar a la nueva franja horaria del usuario. La readaptación de franjas horarias puede conllevar pérdida de información, dado que la RP deberá seguir la configuración dispuesta para poner en función la monitorización y las escuchas esporádicas se darán fuera de los rangos horarios establecidos, es posible que haya un desfase entre adaptación a horario y escucha que produzca esa pérdida de información. Este pequeño inconveniente se ve compensando en que el usuario no se ve obligado a comunicarle directamente al CPS cuando tiene que efectuar mediciones, si no que mediante su rutina se va produciendo esta adaptación. No obstante, dado que una de las maneras de interactuar con el CPS consta de una aplicación que permite configurar ciertas características del sistema, existe la posibilidad de marcar las horas de manera manual, si fuese necesario.

Para finalizar con este capítulo se presenta el último tema que atañe al diseño y construcción del CPS, la seguridad. Tras el análisis y revisión del listado de ataques a los CPS de las tablas 3.1 y tabla 3.2 se aprecia que estos

están clasificados según la capa del CPS que afecte. La tabla 3.2 se centra en los ataques DoS y en las redes de sensores. Por un lado se puede ver que en función de qué capa del sistema se trate, hay más o menos modalidades de ataques. Por otro lado esta lista está basada en ataques de DoS, ya que el trabajo de (Khattak et al., 2019) reseña que es la principal amenaza de dispositivos IoT que cuentan con sensores. Este tipo de ataques consiste en negar el uso de una red o una computadora a un usuario legítimo mediante la saturación o sobrecarga por peticiones de recursos o servicios que se realicen en este sistema (Mirkovic y Reiher, 2004). En un entorno como el presentado, lo que pretenden estos ataques es saturar la comunicación entre el sensor y la placa, de manera que se procesen tantas falsas señales que el sistema se sature y no pueda continuar procesando señales correctas. Dado que esto supone un compromiso al sistema, y aunque no supone un riesgo extremo para la vida del usuario pero sí para su monitorización, es un ataque que demanda alta importancia y por ello se ha decidido trabajar sobre él. Otra razón por la que se ha decidido trabajar sobre los ataques DoS, es por abarcar mayor seguridad en varias partes del sistema, es decir, los ataques DoS pueden afectar a varias capas del sistema, así que brindando una protección mayor al sistema la posibilidad de reducir daños se incrementa.

La respuesta que se presenta en el contexto de esta tesis a estas amenazas consiste en un simulado de nuestro CPS enfocado a los ataques DDoS. El simulador es un modelo basado en agentes que permite la interacción de ataques con el sistema de una manera segura. El simulador permite definir varios agentes que pueden cumplir el rol de atacantes, peticiones normales hechas por un usuario y el mismo sistema, una consecuencia directa de este tipo de simuladores es permitir la simulación de ataques DoS y DDoS. Los agentes que cumplen el rol de atacantes pueden ser configurados con ciertas características propias de los ataques, como duración del ataque, cantidad de atacantes y la manera de cómo se coordinan o efectúan oleadas de ataques. Una de las principales ventajas de este simulador y que favorece la anticipación en el sistema real, es que de la misma manera que se pueden definir estrategias de ataque DDoS, permite establecer estrategias de defensa. La confrontación de estrategias arroja un dato bastante relevante que consiste en la tasa de peticiones atendidas a agentes normales reales y agentes atacantes, de manera que se pueda establecer el método más idóneo ante una determinada amenaza o grupo de estas. Desarrollando estrategias de defensa podemos aportar un extra de seguridad a varias capas del CPS, además los ataques de DDoS se ajustan muy bien a CPS que incluyen sensores, al fin y al cabo una señal de apertura o cierre es registrada por una placa de procesamiento y traducida a lenguaje máquina como “uno” o “cero”, así que lo ideal sería prevenir a nuestra placa de recibir una cantidad constante de mensajes erróneos y esta colapse.

El siguiente capítulo se centra en los detalles del CPS y explica de una manera más técnica como ha sido construido, para ello se apoya de las publicaciones presentadas en revistas de alto impacto.

Capítulo 4

Discusión integradora de artículos resentados

Este capítulo describe las publicaciones editadas que se aportan, así como una discusión de cómo en ellas se cubren los principales objetivos de investigación planteados en esta tesis doctoral. Estos artículos describen los distintos aspectos del CPS propuesto y cómo fueron incorporándose a éste las distintas características y adaptaciones al usuario. Este capítulo consta de varias secciones que reflejan las líneas de trabajo planteadas desde la sección 3.1.1 hasta la 3.1.5.

4.1. Componente físico del CPS.

En la sección 3.1.1 se plantea la cuestión de cuál sería el soporte físico más adecuado para un CPS en el entorno del hogar, y aunque ya se ha mencionado que el soporte es un armario, en la presente sección se aportan datos que afianzan esta elección. En el artículo 6.1 “Collaboration of Smart IoT Devices Exemplified With Smart Cupboards” se propone el primer prototipo de armario (ver figura 4.1), el cual ya considera el hardware necesario para poder realizar monitorizaciones al usuario, a pesar de que el objetivo del artículo citado era validar la aceptación por parte de los usuarios con dispositivos IoT mediante una aplicación y esta ha resultado ser positiva, descubrimos que el prototipo funcionaba bien, pero este no era adecuado para realizar pruebas de cara a la monitorización del usuario.

En el artículo 6.2 “Smart Cupboard for Assessing Memory in Home Environment” se propuso otro modelo de armario para cubrir las carencias del anterior y este fue el finalmente usado. El motivo de la elección de este armario era validar de manera más fiable la monitorización del usuario. El prototipo principalmente propuesto presentaba inconvenientes, uno de ellos



Figura 4.1: Primer prototipo del Armario

es que este armario solo poseía dos puertas, por lo que los posibles resultados que se obtengan de los experimentos no serán relevantes. El problema de dos puertas es que con los resultados obtenidos no podemos determinar cualquier cosa que se requiera medir, ya que los resultados no podrán ser diferenciados de resultados obtenidos al azar. Además, existe otro inconveniente con el prototipo, y es que si el usuario ha de interactuar con el contenido de este mediante búsquedas, una vez que abra uno de los dos compartimentos el contenido del compartimento de al lado es visible ya que no existe una barrera que impida separar el contenido de un compartimento a otro.

Como observamos en nuestra investigación del artículo 6.2 resultó efectivo tener tres puertas, mayor al número de puertas del prototipo inicial debido a que resolvían problemas primerizos en el prototipo. Incluir un método de barrera que impidiera al usuario ver el contenido del compartimento contiguo no resolvía totalmente los defectos del prototipo inicial. El prototipo presenta otro problema, y es que cuando el usuario abre un compartimento, este se encontraba dividido por una balda horizontal, y esto dificulta bastante la monitorización del usuario, ya que no se puede saber a ciencia cierta con qué elementos está interactuando el usuario. El motivo del comportamiento descrito es que se trata de un compartimento de dos cajones. Este tipo de compartimento está dividido de manera que cuando el sensor de la puerta indique que este ha sido abierto, podemos saber a qué conjunto de elementos se está refiriendo, pero no con la suficiente precisión que nos gustaría. Si existe una clasificación de alimentos entre compartimentos superiores e inferiores, no podremos hacer que nuestros análisis cuenten con esa precisión



Figura 4.2: Foto del armario final

para la monitorización del usuario.

Una vez detectados todos estos inconvenientes en el prototipo inicial, el siguiente modelo, y definitivo, es el que se muestra en la figura 4.2. Este armario posee varios compartimentos individuales de manera que podemos saber más precisamente de qué compartimento sale un elemento o alimento. Los compartimentos a pesar de que son contiguos poseen “barreras” de madera que impiden ver lo que hay en los compartimentos de los lados. De vuelta al artículo 6.2, este modelo fue usado para realizar pruebas con 23 voluntarios a los que se les pidió interactuar con el de varias maneras para poder determinar si el CPS propuesto era capaz de medir la memoria.

Los resultados que se obtuvieron, determinaron que el CPS es capaz de medir la memoria, y en cuanto al componente físico el investigador principal de la prueba observó que todos los voluntarios fueron capaces de terminarla y el componente no fue un impedimento. Cada voluntario pudo extraer y buscar los elementos requeridos sin ningún problema, además no tuvieron que aprender a usar el armario ya que al tratarse de un elemento doméstico cada voluntario ya poseía interiorizado su uso.

El número de compartimentos que tiene el armario de la figura 4.2 son tres, los cuales ayudan a obtener datos más precisos en la monitorización del usuario. Con dos compartimentos era difícil discernir qué aciertos podrían ser producidos al azar por parte de los voluntarios en las pruebas. Para apoyar esta afirmación, el artículo 6.2 presenta una correlación de pruebas,

	Componente	Precio
1	Raspberry PI 3B+	44,50
2	Sensores de puertas (3 pares)	5,97
3	Placa de prototipado	4,99
4	Cableado	6,99
	Total	62,45

Tabla 4.1: Precio de los componentes hardware del CPS

ambas hechas por voluntarios, una de ellas es la extracción de productos del armario y otra con un test conocido de medición de memoria. Estas correlaciones fueron hechas mediante la correlación de Pearson y el coeficiente de Kendall (Benesty, et al. 2009). Los resultados demostraron una correlación significativa y positiva, corroborando así, las afirmaciones previamente realizadas y demostrando la acertada elección del componente físico. Finalmente La tabla 4.1 reúne a manera de resumen todos los componentes hardware de los que está compuesto el CPS a la vez que su precio comercial expresado en euros.

4.2. Interacción con los perfiles de usuarios.

En la sección 3.1.2 se aborda la interacción del usuario con el CPS dejando al aire la pregunta de cómo debe intervenir el usuario en el CPS. Ya que se ha determinado que el soporte físico es un armario de cocina, no pretendemos cambiar la interacción normal con este, es decir que el armario continuará con su función normal de almacenaje. Sin embargo se ha tenido en cuenta otros posibles tipos de interacción que tienen que ver con la configuración del CPS y la interacción natural del armario.

4.2.1. Configuración del CPS

Teniendo en cuenta algunas de las premisas del CPS como dispositivo “low-cost” y fácilmente usable se tiende a pensar que el hardware y los demás componentes del CPS son elementos pequeños y que no van a intervenir en espacios físicos de importancia para el usuario o que su situación no compromete el espacio del soporte físico. No obstante dado que el CPS propuesto tiene un tipo de usuario objetivo que puede que no tenga los conocimientos técnicos necesarios para configurar el sistema como personas de la tercera edad o con alguna incapacidad visual, se ha tenido en cuenta a los cuidadores o familiares como usuarios dispuestos a configurar el CPS para el usuario final.

El artículo 6.1 “Collaboration of Smart IoT Devices Exemplified With Smart

Cupboards” ha llevado a cabo un estudio en el que se evalúa la interacción entre los usuarios y los dispositivos IoT. Para ello una aplicación en la que se deben replicar tareas mediante un avatar fue construida. El manuscrito detalla cómo deben ser llevadas a cabo tareas que impliquen dispositivos IoT e interacción humana. En concreto el artículo se ha centrado en la interacción del usuario con un armario inteligente, para ello ha llevado a cabo un estudio de usabilidad en el que se presentaba un avatar y se le pedía al usuario que replicara una determinada tarea para ser llevada a cabo mediante toques en la pantalla, o arrastrando extremidades del avatar con el dedo. Cuando una de las tareas requeridas era completada con éxito, la aplicación devolvía feedback positivo al usuario, de esa manera el usuario apreciaba que la tarea se había efectuado con éxito.

La usabilidad y adherencia de la aplicación fue validada con la escala de sistema de usabilidad, SUS (Bangor et al., 2008) (por sus siglas en inglés), y el cuestionario de utilidad, satisfacción y facilidad de uso, USE (Lund, 2001) (por sus siglas en inglés). Los cuales mostraron resultados positivos, esto indica que esta es una herramienta idónea y apropiada para que los familiares y cuidadores pueden configurar adecuadamente un CPS en sus hogares mediante el uso de tareas indicadas o más bien mediante el uso de una serie de pasos indicados a través de una aplicación. La ventaja principal de este medio es que las dudas acerca de la configuración de un CPS casero quedarán disipada y el usuario tendrá la confianza de que los componentes, y en principio los componentes hardware, quedarán conectados, funcionando y a punto.

En conclusión, los usuarios con un perfil tecnológico bajo o normal serán capaces de llevar a cabo el montaje de un CPS casero en sus propios hogares. A pesar de que el componente hardware ha quedado establecido, falta la configuración interna del CPS, ya que como es lógico no es suficiente con este montaje.

El artículo 6.3 “PriorityNet App: A Mobile Application for Establishing Priorities in the Context of 5G Ultra-Dense Networks” habla sobre el diseño de una aplicación para establecer prioridades en el contexto de IoT. El artículo aborda la necesidad de una aplicación que sea capaz de sincronizar eventos, servicios o sistemas IoT para la siguiente generación de telefonía móvil, la 5G. El ejemplo más representativo de este escenario se da en los hogares inteligentes o smart homes en los que se posee varios dispositivos inteligentes y el poseedor de estos necesita que estos dispositivos hagan su función de manera serializada o priorizando ciertos elementos. Un ejemplo de esta idea pasa por que primero se active el robot de limpieza, luego el termostato esté a una determinada temperatura y el robot de cocina empiece a cocinar una determinada receta. Por lo tanto esta herramienta es la encargada de configurar el CPS por medio de la intervención del cuidador o familiar.

Profundizando en la herramienta, su interfaz consta de dos columnas una a la izquierda y otra a la derecha. La columna de la izquierda tiene todos los servicios disponibles en forma de iconos, y la columna de la derecha tiene como función establecer el orden de todos los servicios ubicados en la columna de la izquierda. En general la interfaz es muy fácil de usar por parte de los usuarios, como demuestran los resultados de los test SUS y USE del artículo. Los resultados de las pruebas en el test USE y SUS fueron de 82.94% y 72.26% respectivamente, corroborando así la facilidad de uso y el fácil aprendizaje de la herramienta. Como mecanismo más avanzado cabe destacar dos elementos, la automatización de procesos en el CPS y prestaciones futuras.

En relación a la automatización de procesos contamos con aquellos procedimientos que establezcamos nosotros mismos o dejemos establecer al usuario, por ejemplo, si poner en marcha el CPS implica dejar pasar corriente eléctrica de un enchufe inteligente, encender una placa de procesamiento y poner en marcha el script adecuado, es mejor automatizar este procedimiento ofreciendo al usuario un único ítem que se denomine “iniciar” a ofrecerle todas las opciones que probablemente le cueste recordar. Si es el usuario el que establece el orden y las prioridades de los servicios gozará de personalizar algunas características del CPS, por ejemplo establecer cuales son las horas prioritarias del día en que el sistema debe estar a pleno rendimiento y cuales debe estar en reposo. Como se explicará más adelante, estas franjas horarias son seleccionadas automáticamente, pero mientras el algoritmo se adapta a la rutina del usuario es buena opción ofrecer la capacidad de variar estas franjas horarias.

El mecanismo avanzado para prestaciones futuras con esta aplicación tiene en cuenta el sistema en su totalidad y a todos sus componentes. En un futuro escenario y teniendo en cuenta componentes ya presentes como una placa de procesamiento y futuros componentes como un altavoz inteligente, es obvio pensar en explotar servicios que estos elementos puedan brindar de cara al futuro. Una vez que el núcleo del CPS ya esté definido no estaría de más añadir tareas personalizadas que deriven de los componentes del CPS, como por ejemplo poner en marcha una lista de música, priorizar elementos del armario para una futura compra en caso de que el CPS detecte la ausencia de algunos de estos elementos.

En materia técnica y sin distinguir mecanismo de interacción, cada elemento de la pantalla de prioridades de la aplicación está compuesto por conjuntos de atributos fácilmente compartibles entre sistemas y en formato JavaScript Object Notation (JSON) como muestra la figura 4.3.

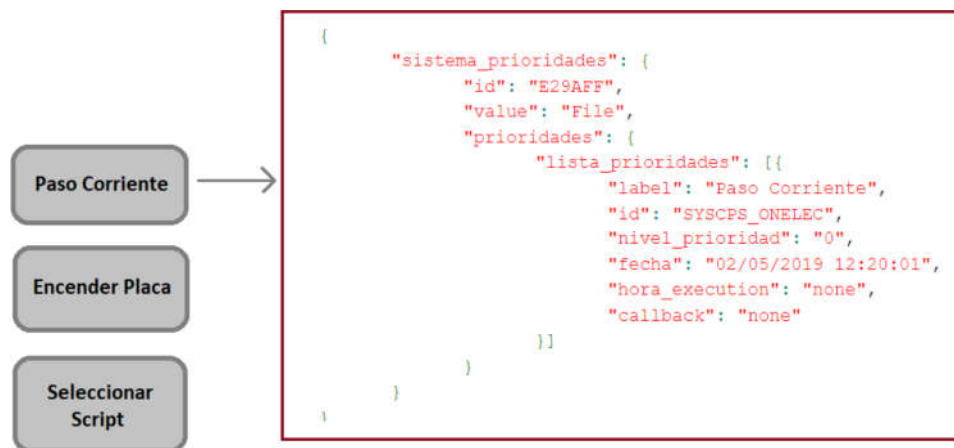


Figura 4.3: Ejemplo del contenido de cada elemento de la aplicación en formato JSON

La ventaja de usar JSON es que es un formato de texto creado para el intercambio de datos y comunicación de sistemas, además es muy fácilmente editable ya que se pueden borrar y añadir tantas líneas como se desee. En la figura 4.3 se ve como ejemplo tres elementos que pueden ser ordenados o priorizados, concretamente es el ejemplo de automatizar el método de iniciar el CPS. La imagen también ilustra la información en formato JSON de cada elemento. La información relevante que es observable es la siguiente: **label** el cual contiene la etiqueta que presenta el botón que vemos a la izquierda, **id** para categorizar la acción que debe llevar a cabo el sistema, **prioridad** que indica cuán prioritaria es esta acción en relación a las demás, **fecha** registro de cuando se ha enviado esta acción, **hora_execution** si fuera necesario indicar una hora para ejecutar esta acción este campo se encargaría de guardarla y finalmente el campo **callback** guarda el nombre de una callback si fuera necesaria ejecutarla en algún sistema remoto. Los dos últimos campos están presentes pero no se usan actualmente, se han incluido teniendo en cuenta futuras prestaciones del sistema.

4.2.2. Interacción natural con el usuario

La interacción natural con el usuario no tiene ningún aspecto realmente impresionante, ya que como se ha mencionado, esta no debe cambiar a menos que la ganancia que se obtenga con este cambio sea funcional, sirva realmente al usuario y por supuesto que no entorpezca una actividad rutinaria y normal como abrir el compartimento de un armario. Sin embargo, dado que el CPS ha de monitorizar al usuario de manera constante mediante su uso normal, ha de requerir un mecanismo para ello.



Figura 4.4: Sensores de puerta

El soporte físico del CPS dispone de tres pares de sensores magnéticos. Cada sensor puede ser dividido en dos, de manera que este emite un tipo de señal cuando están juntos y otra señal cuando están separados. Una parte del sensor está anclada a la puerta del compartimento y la otra está en el marco interior del compartimento, por lo que si un usuario abre una puerta del compartimento el sensor se separa y emite la señal de apertura, de la misma manera cuando un compartimento se cierra, permitiendo la correspondiente emisión de señales y por consiguiente la monitorización del usuario.

Con este mecanismo se puede llevar a cabo un estudio de patrones o de la memoria como se explicará más adelante. Los sensores que se han usado para el CPS actual son los que se muestran en la figura 4.4. Estos sensores van conectados a la placa de procesamiento de manera que las señales puedan ser recibidas y tratadas por ella cuando el usuario interactúa con el armario mediante aperturas o cierres.

4.3. Monitorización técnica del CPS al usuario.

En la sección 3.1.3 se ha planteado la cuestión de qué característica va a monitorear el CPS y cuál iba a ser la manera de hacerlo. De manera resumida la característica a monitorear es la memoria del usuario con la finalidad de detectar pequeños olvidos que podrían ser señales de signos prematuros de

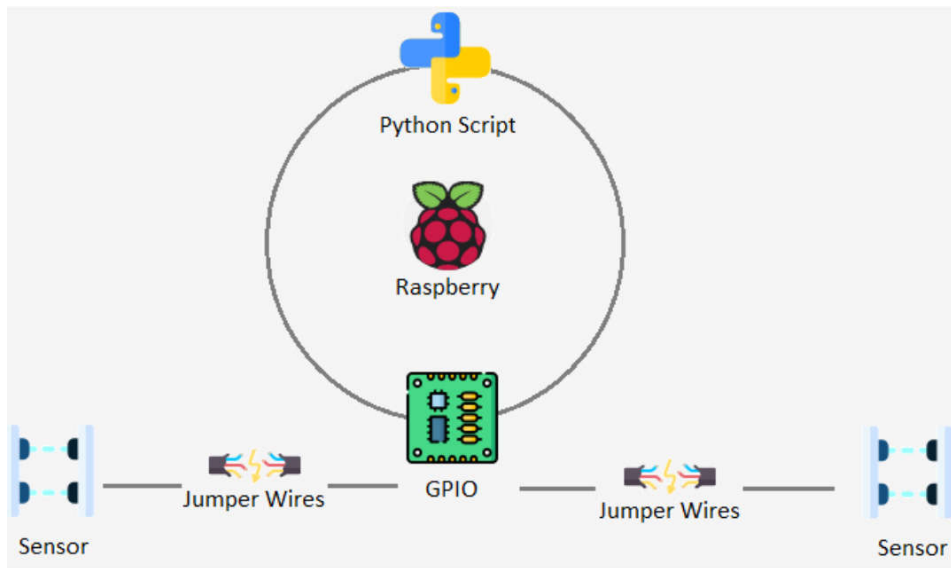


Figura 4.5: Mecanismo técnico del CPS para detectar olvidos

la enfermedad del Alzheimer. El artículo 6.2 centra sus esfuerzos en ello mediante una Raspberry PI modelo 3B+ como placa procesadora. El artículo detalla cómo se reciben y analizan las señales de apertura que genera el usuario cuando abre uno de los compartimentos del armario. La figura 4.5 resume el mecanismo instalado en el CPS.

En primer lugar cada sensor consta de un par de cables que han de ir conectados a la RP mediante el puerto de propósito general de entrada/salida o GPIO (por sus siglas en inglés). Dado que los cables de los sensores no encajan con los pines del puerto GPIO se han usado cables de puente (en inglés jumper wires) para que puedan encajar en los puertos GPIO, además que sirven de extensores de cable para aquellos sensores que están muy alejados de la RP.

La RP contiene un sistema operativo (SO) llamado Raspberry Pi OS (anteriormente conocido como Raspbian) el cual está basado en una distribución Debian. Gracias a este SO se pueden ejecutar diferentes programas. Se ha desarrollado un script, que se pone en marcha en el SO, y el cual se encarga de recibir todas las señales de los sensores. El script siempre está a la escucha de los sensores, por lo que su funcionamiento dependerá de que la RP este en marcha.

En cuanto al diseño del script, este se encarga de recibir las señales que le proveen los pines del puerto GPIO al que están conectados los sensores. Dado que los pines están clasificados mediante una determinada numeración

indicada en la documentación de la RP es fácil saber que pines se deben escuchar. Para llevar a cabo la medición de la memoria, el diseño del script ha tenido en cuenta las siguientes reglas:

1. Se ha de llevar un recuento de las veces que el usuario abre un compartimento del armario, al igual que también ha de llevar un recuento de las veces que ha fallado y ha acertado en la búsqueda.
2. Para determinar un fallo en la búsqueda, el sistema comprueba cada vez que se abre un compartimento y se cierra, en ese momento se añade un intento fallido al contador de intentos fallidos. Una vez se cierra el compartimento y tras el paso de un tiempo prudencial el contador de fallos resta una unidad y el de aciertos suma una unidad. Indicamos que es un acierto y no es un fallo, ya que el comportamiento del usuario da a entender que ha buscado algo en el armario y lo ha encontrado, ya que no ha vuelto abrir ese compartimento o ningún otro.
3. Una vez que se abre un compartimento se marca un fallo y se pone en marcha un contador de tiempo, de manera que se determine cuando el usuario ha dejado de buscar. Si aún no ha pasado un tiempo prudencial, y el usuario abre un compartimento y lo cierra, el contador de fallos vuelve a aumentar en una unidad los fallos, ya que si el usuario abre otro compartimento la búsqueda del objeto deseado ha fallado en el primer compartimento. A partir de aquí todo se resuelve como el punto 2.
4. La última regla de diseño que se ha tenido en cuenta para el script tiene en cuenta la posibilidad de que el usuario presente síntomas avanzados de la enfermedad. Cuando un usuario abre un compartimento, ocurren las acciones que antes se han comentado, sin embargo se pone en marcha otro contador, el cual tiene en cuenta el tiempo de búsqueda del usuario, este contador está en marcha mientras el compartimento en el que actualmente se está efectuando una búsqueda permanece abierto. Si después de un determinado tiempo el compartimento sigue abierto, añadimos una unidad al contador de fallos. Este fallo es interpretado como que el usuario ha olvidado que estaba buscando.

A medida que se van obteniendo fallos y aciertos, las aperturas son almacenadas y cuando estas alcanzan un determinado umbral se efectúa una evaluación sobre la tasa de fallos y si esta alcanza un porcentaje considerado alarmante se informa al usuario que visite a un médico experto en la materia.

Como apunta el artículo 6.2 este método de monitorización de la memoria ha sido probado con 23 participantes obteniendo resultados muy destacables

como la capacidad de medir la memoria. Sin embargo, la duda acerca de la validez del método puede causar ciertas dudas, es decir cómo podemos afirmar que este método realmente mida la memoria de los usuarios. En colaboración con la doctora Rebecca Amariglio de la Universidad de Harvard y del Massachusetts General Hospital, coautora del artículo, se establece validar los resultados de las pruebas obtenidas con otros métodos ya conocidos y validados de medir la memoria, por lo que una prueba de caras y nombres fue lo más apropiado.

La prueba de caras y nombres consiste en presentarle a cada individuo un determinado rostro de una persona asociado a un nombre, de manera que pueda memorizar una cara con un nombre. Sin embargo el tiempo que dispone para memorizar los pares de caras y nombres es limitado y la cantidad de pares que se usan para tal estudio puede llegar a superar la veintena. Una vez que se ha llevado a cabo la memorización, el participante vuelve a ver uno de los rostros presentados y se le pide que diga su nombre de manera que al final se puedan contabilizar aciertos y fallos. Es de destacar que la prueba de caras y nombres fue usada en (Rentz et al., 2011) para demostrar la relación entre el deterioro de la memoria y la beta amiloide.

Retomando el tema del CPS una vez que los participantes realizaron pruebas con el armario, luego realizaron una prueba de caras y nombres. Los resultados obtenidos de esta prueba fueron cruzados con los resultados obtenidos de la prueba del CPS. El cruce de resultados demostró que existía una correlación estadísticamente significativa, lo que confirma que el CPS es capaz de medir la memoria y a pesar que no se ha sometido el CPS al estudio del deterioro de la memoria como en (Rentz et al., 2011), al menos la relación entre ambas pruebas arroja ciertos indicios de que el CPS pueda ser explotado en esa dirección.

4.4. Modelo de alimentación eléctrica.

En este punto de la tesis ya es factible saber como interactúan los componentes que conforman el CPS. El único elemento que necesita recibir una fuente de alimentación constante es la placa de procesamiento RP. Los sensores no necesitan de una alimentación energética directa ya que estos se alimentan de la corriente eléctrica que es proporcionada por la RP.

La cuestión energética es planteada pensando en que aunque el consumo energético no es excesivo, si que es constante. Además, para que el CPS siempre pueda atender las peticiones del usuario sus componentes deben estar conectados a la corriente eléctrica..

La RP cuenta con un modo de suspensión como otros sistemas operativos como Windows, o Linux, o incluso como otros dispositivos comunes como teléfonos móviles o smartbands, así que para dar una respuesta a la cuestión del consumo eléctrico, planteada en la sección 3.1.4, de este componente, se propone un algoritmo basado en el comportamiento y rutina del usuario para tener todo el sistema en marcha y tener el sistema con las necesidades mínimas para estar en funcionamiento. El artículo 6.4. “Green Communication for Tracking Heart Rate with Smartbands” expone el estudio de la frecuencia cardiaca tomada mediante una pulsera inteligente. En el artículo se monitoreo la frecuencia cardiaca de un sujeto de pruebas durante 3 meses de manera que fue capaz de detectar los días y los momentos del día en el que se registraba una frecuencia cardiaca anormal, ya sea por debajo de las 60 pulsaciones por minuto (ppm) o por encima de las 120 ppm.

Registrando la rutina del usuario y los rangos horarios de posible riesgos es fácil establecer los periodos en los que un dispositivo IoT o un CPS debe estar a pleno funcionamiento o debe estar en modo de suspensión o ahorro de energía. El artículo registraba la rutina del usuario mediante la frecuencia cardiaca, en el caso de CPS propuesto, esta rutina se registra mediante el uso del armario, dado que este posee sensores en la puerta de los compartimentos y las aperturas son registradas, bastaría con establecer un rango horario como lo propone el artículo para establecer las frecuencia horarias de funcionamiento, que a priori podrían coincidir con la hora del desayuno, comida y/o cena.

El artículo no obviaba el hecho de que un sujeto pudiese cambiar de rutina, por ejemplo se registró que el sujeto de prueba marcaba pulsaciones anormales todos los jueves entre las 20:30 y las 22:00 de manera que la smartband sabía en qué momentos debía estar a pleno rendimiento. Además de esto, y una vez establecido el plan de monitoreo, la pulsera permanecía a la escucha de estas mismas situaciones y las comparaba con el horario que ya tenía establecido de manera que cuanto menos coincidía con los rangos establecidos, este algoritmo se iba adaptaba al nuevo horario. Esto es algo totalmente lógico, ya que el usuario de a pie puede cambiar su rutina por causas mayores o por deseos propios.

En conclusión, la intervención energética que se propone para el CPS es el uso de un algoritmo adaptativo basado en la rutina del usuario, para que la RP entre en estado de suspensión y activación en función de rangos horarios basados en los usos que se haga del CPS.

4.5. Seguridad en el CPS: Simulador ABS-DDoS.

Dado que todos los puntos anteriores ya han sido definidos y sobre todo puntos cruciales como los componentes hardware y componentes software, queremos señalar en este apartado cuáles son las cláusulas destinadas a la seguridad del CPS. En la sección 3.3 ya adelantábamos cual era la repuesta a la aportación en materia de cyber seguridad, por lo que esta sección reafirma esta elección exponiendo las principales cualidades del simulador con la publicación editada.

En dicha sección los ataques más comunes fueron listados y clasificados según el tipo de componente usado para la recolección de datos, ya fueran RFID o WSN. Dado que el presente CPS no usa ningún RFID y las aperturas del armario son controladas por sensores, la presente resolución tendrá en cuenta los ataques DoS que actúan sobre las WSN como objeto de estudio. Dado que el CPS se encuentra en una etapa inicial una solución particular a cada tipo de ataque no sería lo más idóneo para adentrarse en aspectos de seguridad, así que lo más adecuado en estas circunstancias es una solución general a los ataques de DoS.

El artículo 6.5 "ABS-DDoS: An Agent-Based Simulator about Strategies of Both DDoS Attacks and Their Defenses, to Achieve Efficient Data Forwarding in Sensor Networks and IoT Devices" aborda el tema de seguridad anteriormente mencionado. Antes de entrar en detalles el artículo se centra en los ataques de denegación de servicios distribuidos pero su contenido es fácilmente adaptable a los ataques DoS ya que ambos ataques tienen la misma finalidad, la de dejar inservible o inactivo un sistema. La principal diferencia entre ambos es que el DDoS se efectúa desde varias máquinas al mismo tiempo, haciendo que la saturación en la máquina objetivo sea aún mayor y el ataque DoS se efectúa sólo desde una máquina.

El artículo se basa en el diseño de un modelo basado en agentes (MBA) el cual trata de un entorno controlado de simulación de individuos autónomos y ver cómo se comportan entre ellos bajo unas premisas dadas (Izquierdo et al., 2008). Este MBA permite simular mediante agentes el sistema o máquina objetivo, lo que viene siendo el CPS propuesto y que va a ser objeto de ataque y una máquina atacante es decir la que efectúa ataques DoS. Aparte de estos dos agentes el ABS-DDoS, nombre que se le ha dado al MBA, permite definir otros tipos de agentes, como agentes honestos, los cuales representan peticiones reales de usuarios reales. Otro agente importante es el agente observador, el cual no tiene actuación directa en el acto, sino que se encarga de observar y recolectar datos de todos los agentes con la finalidad de arrojar datos cuantificables que permita valorar la simulación.

La función principal del ABS-DDoS es permitir la simulación de estrategias de defensa contra ataques de DoS de manera que se puedan valorar que tan bien funcionan. Dado que una estrategia de ataque de DoS puede tener un patrón determinado, por ejemplo que se realicen muchas peticiones para bloquear el sistema cada ciclo de segundos, sería fácil detectar este comportamiento y bloquear las peticiones hechas por los atacantes que se reciban, con una adecuada estrategia de defensa. Es lógico pensar que una estrategia de ataque no tiene porque tener un patrón sencillo o fácil de descifrar, por esa razón mediante el ABS-DDoS se pueden definir estrategias de ataque personalizadas al igual que estrategias defensas. Ambas estrategias son enfrentadas y se obtiene una tasa de peticiones rechazadas a atacantes y peticiones rechazadas a agentes honestos, siempre intentando obtener una tasa alta de rechazo para atacantes y baja para los honestos.

Es difícil predecir de qué manera el CPS propuesto puede ser atacado, en relación a ataques DoS, dado que se encuentra en su etapa más temprana y como es lógico se desconoce el modo de actuar de los atacantes, sin embargo ABS-DDoS es una herramienta que nos permite adelantarnos, a priori, estableciendo estrategias de defensas contra las maneras de atacar más frecuentemente usadas. En el caso de detectar un ataque a nuestro CPS que no concuerde con ninguna de las estrategias propuestas, este puede ser simulado y estudiado para adoptar la mejor estrategia de defensa.

Teniendo en cuenta que el artículo 6.5 se adapta para hacer frente a los ataques de DoS, en el momento de que los servicios del CPS escalen o que el mismo CPS escale a un ámbito más grande, la probabilidad de sufrir ataques de DDoS incrementarán. Una vez que la escala se da, no hace falta adaptar ningún simulador, y se podrá usar el que el artículo describe por defecto, el cual hace frente a los ataques DDoS. La susceptibilidad a los ataques DDoS viene dada por servicios remotos como dar a conocer la evolución de la memoria de un potencial enfermo de Alzheimer a sus familiares, o dar a conocer el contenido del CPS en tiempo real.

Finalmente, dado que los MBA permiten simular entornos controlados mediante agentes, si el CPS sufre un ataque de otro tipo, siempre es posible readaptar el ABS-DDoS para el estudio de dichos ataques, obteniendo como consecuencia la estrategia más adecuada para defender el sistema, ya sea en cuanto a peticiones atendidas, tiempo empleado o recursos utilizados. Además el simulador ABS-DDoS nos permite establecer estrategias robustas frente a ataques de DDoS para que nuestro CPS pueda dar servicios en remoto repeliendo todo tipo de ataques.

El siguiente capítulo presenta todas las conclusiones finales obtenidas con la elaboración de esta tesis y del CPS por consiguiente. También se destaca

las líneas de trabajo futuro, cuyas ideas se centran en expandir y explotar más servicios que pueden ser añadidos a un CPS como el aquí presentado.

Capítulo 5

Conclusiones y trabajo futuro

Sectores de la sociedad de hoy optan por evadir o tratar temas como el sufrimiento, enfermedad, o lo que esto quiera significar y esto puede ser un error. Vivimos con menos enfermedades que nunca, siempre echando la vista atrás, y el estado de bienestar de muchos países desarrollados es bueno y estable. No obstante, no es tan malo que convivamos con las enfermedades. Es algo que está ahí, que nos va a pasar antes o después y por lo tanto tenemos que soportarlo cuando llega. Por lo que educar a la gente en que nuestra cultura y el mundo en el que vivimos es finito, y en él que hay que morir, es un proceso idílico, concluyente y que aunque no es objeto de esta tesis, al menos pretende transmitirlo. Así que hay que educarse para la enfermedad o más bien educarse para la muerte ya que es algo que nunca se podrá evitar

El aumento de la esperanza de vida viene acompañado de una mayor prevalencia de enfermedades neurodegenerativas, una serie de trastornos del sistema nervioso que a día de hoy están siendo considerados entre las principales causas de mortalidad. Provocadas por un aumento en los procesos de muerte celular, y la consecuente reducción del número de neuronas, estas enfermedades desencadenan alteraciones en muchas actividades y funciones corporales como el equilibrio, la movilidad, el habla, la respiración o la función cardíaca. Entre ellas, las más frecuentes son, el Alzheimer y el Parkinson, ambas asociadas a la edad. Para desdicha de muchos, aún no existe una cura efectiva para ambas enfermedades, y nos consta con la elaboración de esta tesis que la comunidad científica está dividida en dos grandes grupos. Uno de ellos es el que centra sus esfuerzos en combatir y erradicar dichas enfermedades. El otro grupo, en el cual nos enmarcamos, nos dedicamos a que aquellas personas que las padecen lleven de la mejor manera su enfermedad. Proyectos como estos aportan una pequeña materia en este sector que puede ser aprovechado por los pacientes u otros compañeros científicos.

Concretamente, esta tesis aporta a las personas sin ninguna patología el

control y monitorización de los procesos mentales que repercuten en enfermedades más graves, de manera que la detección de estas se efectúen de la manera más precoz. Con la pronta diagnosis las personas aprenderán a convivir con la enfermedad de la manera más soportable posible. Nos gustaría concluir con esta parte indicando rotundamente que la monitorización del usuario tiene un impacto directamente positivo en el usuario, ya que la diagnosis se efectúa correctamente, sin embargo este es un proceso que se prolonga mucho en el tiempo lo que lo hace difícilmente observable. Lo que sí podemos afirmar es que esta herramienta es una más de las opciones con las que puede contar el usuario para el proceso de diagnosis.

A través de esta tesis se han realizado varias contribuciones en el área de los CPS aplicados a la salud. El objetivo de esta tesis ha sido explicar de manera concisa y detallada el proceso de elaboración de tales sistemas en el campo de la salud. Para ello esta tesis ha planteado una serie de hitos listados en la sección 3. Dichos hitos trataban de establecer el soporte físico más adecuado para instalar un CPS, establecer la maneras de interacción con los usuarios, establecer los elementos a monitorizar para una posterior estimación de problemas de salud, estimar medidas de seguridad adecuadas y presentar modelos de eficiencia energética para un gasto eléctrico eficiente.

El fruto de la resolución de todos estos hitos es el CPS que hemos denominado armario inteligente de cocina. Su principal característica es el seguimiento y monitorización de la memoria de los usuarios. La contabilidad de los fallos en las búsquedas del armario permite estimar niveles de riesgo que pueden acarrear enfermedades neurodegenerativas, por lo tanto el usuario puede estar controlado mediante el uso de este mismo e incluso advertido ante cualquier riesgo. Este CPS ha sido validado en 23 participantes con un amplio rango de edad (entre 18 y 60 años) en un entorno controlado. Mediante pruebas cruzadas se comparó el test de medición en un entorno controlado y un test bien conocido de caras y nombres. Los resultados demostraron una correlación estadísticamente significativa entre ambos test, permitiéndonos afirmar que el CPS es capaz de medir la memoria y alertar de cuando el usuario presenta olvidos de manera destacable.

Tras un profundo análisis sobre el componente físico más adecuado para desplegar un CPS, se tuvieron en cuenta muebles caseros como las sillas, las mesas, las camas y los armarios. Finalmente y tras verificar determinadas cualidades, establecimos que el armario de cocina es el mueble más adecuado para desplegar un CPS en el hogar bajo las premisas establecidas. Sin embargo es comprensible que esto suscite un gran debate al lector, ya que es de conocimiento público la existencia de sistemas similares. No somos ajenos a que existen muebles con ciertas características que hagan de él un CPS. Sin ir más lejos en el ámbito comercial existen camas inteligentes a dispo-

nibilidad del público. La compañía Reverie con sede en Michigan se dedica a la elaboración de este tipo de productos. Algunas de las características más destacables son: almohadas con lector de ondas cerebrales que recopilan datos para ofrecer feedback al usuario, emisor de ondas de sonido solo para una de las personas de un lado de la cama con el objetivo de ayudar a un descanso más reparador y placentero. Mapa de presión que indica al usuario sus posturas o como esta durmiendo. Adicional a esto la cama inteligente de Reverie posee una interacción por voz gracias a un dispositivo de Alexa, de esta manera aunque esta cama posea aplicación y botones para interactuar con ella se puede apreciar como la tendencia en este tipo de sistemas es incluir interacción inclusiva y pensada para el confort. Ahora bien, tampoco es ajeno para el público en general el valor de este tipo de sistemas. En la página web se pueden ver los modelos más económicos por 3.600 dólares, fuera del concepto low-cost. Por lo que como primera conclusión apuntamos que la holgura de la investigación va marcada por el investigador, sus recursos y sobre todo el usuario objetivo.

La interacción es un componente en el que hemos puesto especial interés dado que uno de nuestros objetivos era que el usuario adquiriera adherencia al uso de nuestro sistema, por lo tanto la manera de interactuar debe ser simple. A través de diferentes análisis realizados a los usuarios en las fases de experimentación destacamos los test SUS y USE que indicaron los niveles de facilidad de uso de nuestras herramientas de interacción e indicaba que íbamos por el “camino correcto”. Dada la buena respuesta obtenida de los análisis, se pudieron obtener formas de interacción adecuadas mediante procesos iterativos que aportan ideas frescas e innovadoras a la vez que suprimen elementos sin sentido o que entorpecen operaciones. Básicamente la interacción ha sido diseñada manteniendo un adecuado equilibrio entre utilidad, usabilidad y buen gusto o lo que en el contexto de marketing denominan como Look and Feel. De cara a un CPS como el presentado en la actual tesis, y quizás cualquier otro CPS, los requerimientos de interacción han de tener muy presentes las necesidades del usuario. Dado que este tipo de CPS se centran en problemas muy concretos, el método de interacción ha de tener una herramienta diseñada acorde a los requerimientos concretos. Además, partiendo de la premisa de que los usuarios objetivos sean personas con pocos conocimientos informáticos o poca adherencia no podemos hacer que ellos mismos sean los responsables de la configuración del CPS. De esta manera esta función quedará delegada en alguien con los conocimientos adecuados o los mismos cuidadores de personas con problemas de salud. Este perfil de usuarios soporta un tipo de interacción más cargada en cuanto a opciones, ya sea porque tenga previo conocimiento o que las probabilidades de que interactúe con dispositivos electrónicos como un teléfono móvil sean altas. Concretamente la interacción que ofrece la aplicación creada para ello ha demostrado un alto nivel de usabilidad y especialmente es fácil de usar.

Además, su escalabilidad es adecuada en términos de cantidad de ítems que pueden ser utilizados para la configuración del CPS.

Llegados a este punto nos gustaría añadir como segunda conclusión que, el diseño de un CPS puede tener distintos niveles de interacción, siempre subordinados por la complejidad de este y de los usuarios protagonistas. Además, se han de seguir teniendo en cuenta conceptos básicos de la IPO y deben ser ajustados a cada necesidad de interacción y usuario.

Durante la revisión del estado del arte, nos dimos cuenta cuan interiorizado está el concepto de industria 4.0 y los CPS. Uno de los ejemplos más notorios es un CPS formado por: sensores inalámbricos, un sistema de alimentación de los sensores por inducción, balizas o sensores de detección de posición, sistema de toma de decisiones, plataforma digital con almacenamiento de datos, sistema de protección contra ciberataques, una pulsera con vibración, gafas de realidad aumentada y un software de ayuda al operario. El CPS trataba de un sistema de fabricación aditiva en el que es importante controlar el nivel de oxígeno para evitar la oxidación del titanio. Este tipo de estructuras incluyen un montaje de tamaño industrial y de maquinaria sofisticada, por lo que a priori el gasto energético es elevado e incluso puede ser más aún cuando el CPS está a pleno rendimiento veinticuatro horas al día. Esta tendencia se ha establecido así porque la industria 4.0 aporta fábricas más sostenibles con un coste operativo lo más ajustado posible en donde prevalece la seguridad de los trabajadores y los mantiene más productivos. Todo ello con el fin de lograr la sostenibilidad empresarial y ser competitivos. Esto no quiere decir, que en la industria 4.0 no se invierta o no se busque la eficiencia energética, todo lo contrario es uno de los campos en los que se incide para destacar frente a la competencia. Lo natural es que los CPS de menor envergadura “hereden” las mejoras energéticas de estos sistemas. Dado que CPS como el propuesto en esta tesis no posee una gran cantidad de componentes, pero si es escalable, podemos decir que se encuentra en el proceso transitivo de incrementar sus servicios, lo que generaría un incremento energético. Mientras este proceso transitivo no avance, damos por adecuado nuestro modelo energético, ya que encaja perfectamente con el perfil de uso del usuario objetivo. Así que en lo que al consumo energético se refiere podemos concluir que este modelo energético es efectivo y adaptable a la rutina del usuario, ya que según el resultado de las simulaciones hechas se ha logrado un ahorro del 85.71% frente a un sistema sin ningún modelo de ahorro de energía y basándose en una rutina diaria de un usuario. Es útil pensar en rutinas o usos puntuales ya que este CPS no requiere un uso a pleno rendimiento de la maquinaria durante todo el día, si no en momentos concretos del día.

Siguiendo en la línea de los CPS dedicados a la industria, los niveles de

seguridad también han de ir acorde a la magnitud del sistema. La industria 4.0 se rodea de elementos tan simples como carteles indicativos hasta consultores propios en ciberseguridad. Teniendo en cuenta el trabajo hecho en la parte de seguridad del enfoque propuesto nos gustaría indicar cual o cuales son los elementos indicados para evitar que nuestro sistema se vea comprometido. Dado que nos hemos centrado en los ataques más populares a las redes de sensores como los ataques de DoS ofrecemos una potente herramienta que permite la simulación de este tipo de ciberataques. Aunque esta herramienta no incide directamente sobre la defensa del CPS, porque no se ha implantado ningún método de prevención de ataques, tiene mucho valor científico, primero por la razón más obvia, que es adoptar correctas estrategias de defensa ante cualquier ataque de DoS, ya que según las pruebas se han cruzado diferentes estrategias de defensa de sistemas y ataques, lo cual ha provisto resultados analizables. Estos permiten discernir al investigador que estrategia es la más adecuada en términos de tiempo y porcentaje de peticiones aceptadas correctamente. La segunda es que favorece mucho el proceso de transición que antes ha sido comentado. A medida que crece un CPS en cuanto a prestaciones y servicios, es normal que otros sectores se vean afectados, y uno de ellos es la seguridad. Si el CPS crece en cuanto a sensores, da la posibilidad de servicios remotos, o incluye una capa extra de gestión de datos ya sea porque controlamos más de un armario o un dispositivo en el hogar, el riesgo en cuanto a seguridad también lo hará. Así que a medida que escala, los comportamientos de nuevos componentes o servicios pueden ser simulados en un entorno hostil y seguir eligiendo la mejor estrategia de defensa para el nuevo estado del CPS.

En conclusión, esta tesis ha presentado el diseño y la creación de un CPS dedicado a la salud haciendo hincapié en sus principales componentes. Las capacidades y limitaciones del CPS también están definidas, sin que esto pueda afectar a limitar futuras ampliaciones de servicios en el CPS. Aunque no es oficial, sí que es obvio ver como expertos en la materia hablan de evoluciones como la transición de IoT a IIoT y de IIoT a entornos inteligente (SE), por lo que no es disparatado pensar que los CPS dedicados a la salud lleven un camino muy parecido.

5.1. Trabajo futuro

Dada las características de un CPS las posibilidades de ampliación son abundantes. Aquí se comentan las más notorias y necesarias teniendo en cuenta la limitaciones del sistema propuesto.

Actualmente nos encontramos trabajando en un sistema de interacción por voz con el armario, de manera que pueda resultarles de provecho a los usua-

rios con alguna discapacidad visual. Hasta el momento se efectúan consultas sobre el contenido del armario con ayuda de un asistente de voz. Sin embargo, una de las limitaciones que tiene el CPS es el proceso de guardar alimentos. Es decir, ya que se ha dado la posibilidad de consultar el contenido en el armario, sería lógico pensar que también se pudiese guardar elementos en el armario. A nivel de interacción de voz esta lógica está creada no obstante, esta operación tiene algunas connotaciones con las que no es fácil lidiar y que merece la pena indagar en ellas. La primera de ellas es que el proceso de guardado tal como está planteada la interacción no supone una acción atómica. Esto quiere decir que convierte un proceso simple en uno más complejo. Un usuario para guardar un elemento en el armario normalmente lo toma, abre un compartimento y lo guarda, por lo que no tiene que especificar ninguna de las características del producto al armario. Esto no es ningún inconveniente cuando se trata de un elemento o dos, pero cuando la cantidad sube a una cifra elevadamente considerable esta operación se torna en algo farragoso. Una opción que merecería la pena explorar es añadir un componente hardware más como una cámara. La cual con ayuda de algoritmos de visión artificial como los que provee OpenCV (Culjak et al., 2012) brinda una solución para un par de inconvenientes.

Por un lado facilita el reconocimiento de formas y objetos, de manera que se registren elementos una primera vez, y las siguientes el usuario sólo necesite confirmación para guardarlo o al menos necesite aportar menos información de la que requiere en un principio. Por otro lado, ayuda aún más al proceso de ubicación de elementos, sobretodo en usuarios con discapacidad visual. Uno de los recipientes que más parecido tiene entre sí son los bricks, por ejemplo la forma de los bricks de leche y bricks de zumos son bastante parecidas. El CPS propuesto solo indica en qué compartimento está guardado un producto, así que si casualmente en un compartimento existen 2 bricks de distintos productos, una persona con discapacidad visual no tendrá la certeza de cuál de los dos productos ha tomado durante una hipotética búsqueda. Así que una manera de identificar estos productos facilitan la operación de búsqueda y aportan más independencia al usuario.

Otro de los servicios que podría extender este CPS es el de llevar una monitorización o control de alimentación, de manera que sea posible gestionar una buena alimentación o incluso llegar a prevenir padecimientos como la obesidad. Sin embargo uno de los principales inconvenientes de este tipo de operaciones va determinado por la cantidad de comida que se pretende ingerir. Si una determinada persona decide preparar macarrones, no está obligado a gastar todos los macarrones de un paquete, primero porque no es algo usual y segundo porque no sabemos si este usuario está preparando macarrones para él, o para varias personas. Dado que no hay una manera de saber las cantidades exactas de comida e incluso una manera amigable de

transmitirlas al CPS, el cálculo de la ingesta de comida no puede efectuarse. Aunque se lograra una manera acorde de calcular las cantidades de ingesta aún quedaría por saber el valor nutricional (i.e. calorías, lípidos y azúcares) de cada alimento. A priori una de las maneras que se ha sopesado es utilizar el código de barras de los recipientes de cada alimento, pero esto supone incorporar más elementos hardware al CPS. El elemento hardware imprescindible es un lector de código de barras que trabaje de manera conjunta con la interfaz de voz para indicarle al CPS el alimento que se extrae, la posible cantidad y con ayuda del código barras se podría realizar un estudio nutricional adecuado.

Siguiendo en el ámbito nutricional, una plataforma digital como soporte para nutricionistas podría ser planteada. En muchos casos cuando un usuario visita al nutricionista este diagnóstica una determinada dieta al usuario en función de las necesidades que demande. Normalmente el nutricionista confecciona una lista de alimentos divididos por días y a su vez clasificados en desayunos, comida y cena. La función de la plataforma digital es permitirle al nutricionista realizar esta dieta como ha sido descrita antes, y que el usuario sea capaz de consultarla al CPS con preguntas sencillas relacionadas con esta. El CPS contestaría con las recomendaciones del nutricionista mediante un altavoz inteligente.

Otra posible línea de trabajo es desarrollar una aplicación móvil que solicite el contenido del armario. Esta aplicación tendría como objetivos iniciales mostrar el contenido del armario, tanto total como por compartimento, esto ayudaría bastante a realizar la típica “lista de la compra”. La otra función es que sería el componente ideal para recibir feedback del CPS. A través de la aplicación se podría visualizar toda la información nutricional sobre la ingesta de comida. Además podría ser una herramienta adecuada para monitorizar parámetros acerca de la información sobre las tasas de olvido provistas por un usuario. Finalmente, se planea valorar si estas funcionalidades pueden añadirse a la aplicación que es usada para configurar el CPS descrita en la sección 4.2.1 o para que sea una aplicación independiente.

El siguiente capítulo, enumera y presenta los artículos publicados en revistas de alto impacto que han servido de eje principal para la elaboración de la tesis.

Capítulo 6

Artículos presentados

A continuación se incluyen los artículos editados que se aportan como parte de esta tesis doctoral.

6.1. Collaboration of smart IoT devices exemplified with smart cupboards.

Cita completa:

GARCÍA-MAGARIÑO, I., GONZÁLEZ-LANDERO, F., AMARIGLIO, R., & LLORET, J. (2019). Collaboration of smart IoT devices exemplified with smart cupboards. *IEEE Access*, 7, 9881-9892.

Abstract:

The variety of smart things connected to the Internet hampers the possibility of having a stand-alone solution for service-centric provisioning in the Internet of Things (IoT). The different features of smart objects in processing capabilities, memory, and size make it difficult for final users to learn the installation and usage of all these devices in collaboration with other IoT objects, hindering the user experience. In this context, we propose a collaboration mechanism for IoT devices based on the multi-agent systems with mobile agents. This paper illustrates the current approach with smart cupboards for potentially tracking memory losses. The user study revealed that users found working products of this approach usable, easy-to-learn and useful, and they agreed that the current approach could provide a high quality of experience not only in the specific case of service-centric IoT devices for tracking memory losses but also in other domains. The learning capability by means of this approach was shown with significant reductions of reaction times and number of errors over the first and second tests with the current approach. System response times were appropriate for both continuous rendering and presenting the classification results. The usage of RAM memory was also adequate for the common actual devices.

Received December 12, 2018, accepted December 22, 2018, date of publication January 1, 2019, date of current version January 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2890393

Collaboration of Smart IoT Devices Exemplified With Smart Cupboards

IVÁN GARCÍA-MAGARIÑO¹, FRANKS GONZÁLEZ-LANDERO²,
REBECCA AMARIGLIO^{3,4}, AND JAIME LLORET⁵

¹Department of Software Engineering and Artificial Intelligence, Complutense University of Madrid, 28040 Madrid, Spain

²Edison Desarrollos, 44002 Teruel, Spain

³Harvard Medical School, Boston, MA 02115, USA

⁴Massachusetts General Hospital, Boston, MA 02114, USA

⁵Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politècnica de Valencia, 46730 Valencia, Spain

Corresponding author: Jaime Lloret (jlloret@dcom.upv.es)

This work was supported in part by the Dpto. de Innovación, Investigación y Universidad del Gobierno de Aragón through the program FEDER Aragón 2014-2020 Construyendo Europa desde Aragón under Grant T49_17R, in part by the University of Zaragoza and the Fundación Ibercaja through the Research Project Construcción de un framework para agilizar el desarrollo de aplicaciones móviles en el ámbito de la salud under Grant JIUZ-2017-TEC-03, in part by the Estancias de movilidad en el extranjero José Castillejo para jóvenes doctores Program, Spanish Ministry of Education, Culture and Sport, under Grant CAS17/00005, in part by the Universidad de Zaragoza, Fundación Bancaria Ibercaja and Fundación CAI, Programa Ibercaja-CAI de Estancias de Investigación, under Grant IT24/16 and Grant IT1/18, in part by the Research Project Desarrollo Colaborativo de Soluciones AAL, Spanish Ministry of Economy and Competitiveness, under Grant TIN2014-57028-R, in part by the Organismo Autónomo Programas Educativos Europeos under Grant 2013-1-CZ1-GRU06-14277, and in part by the Ministerio de Economía y Competitividad through the Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento, under Grant TIN2017-84802-C2-1-P.

ABSTRACT The variety of smart things connected to Internet hampers the possibility of having a stand-alone solution for service-centric provisioning in the Internet of Things (IoT). The different features of smart objects in processing capabilities, memory, and size make it difficult for final users to learn the installation and usage of all these devices in collaboration with other IoT objects, hindering the user experience. In this context, we propose a collaboration mechanism for IoT devices based on the multi-agent systems with mobile agents. This paper illustrates the current approach with smart cupboards for potentially tracking memory losses. The user study revealed that users found working products of this approach usable, easy-to-learn and useful, and they agreed that the current approach could provide a high quality of experience not only in the specific case of service-centric IoT devices for tracking memory losses but also in other domains. The learning capability by means of this approach was showed with significant reductions of reaction times and number of errors over the first and second tests with the current approach. System response times were appropriate for both continuous rendering and presenting the classification results. The usage of RAM memory was also adequate for the common actual devices.

INDEX TERMS IoT, user experience, smart object, collaboration, smart cupboard.

I. INTRODUCTION

Internet of Things (IoT) refers to a paradigm in which smart objects are connected to Internet for providing several functionalities embedded into objects commonly used [1]. Their connection to Internet allows the smart objects to (1) cooperate among them for providing coordinated and intelligent services [2], (2) provide remote control through Internet, and (3) obtain real-time information captured by sensors and send them through Internet.

IoT brings both smart cities and smart homes to life, making intelligent global behaviors possible. In the case of

smart cities, vehicles could connect to the city for (a) finding parking, (b) knowing real-time traffic situations, (c) being warned of temporal danger situations (e.g. obstacle in roads), and (d) knowing where to recharge their electric batteries [3]. Smart homes could (1) alert of emergency situations of elder people to their caregivers, (2) regulate the heating according to presence or common patterns of their inhabitants, and (3) assist people with loss of memories in reminding item locations, events or taking medicines. Smart appliances can also provide functionalities such as remotely displaying the content of the fridge to buy the most convenient food supplies

when the user gets to the supermarket. Even users can plan the cleaning of their house by controlling the cleaning robots through Internet.

In the domain of health and well-being, smart wearable sensors can also collect useful information of users such as their heart rate, their heart rate variability, sugar levels, and the body postures. This information can be useful for example for asking users to slow down for unusual high heart rates [4] or take insulin for inappropriate sugar levels.

Mobile agents are autonomous software entities that can move from one device to another by following the rules of the corresponding multi-agent system (MAS) scenario. In this way, the software can be transferred through different devices to conform a distributed system.

In this context, the current work proposes to use mobile applications for gamifying the learning experience of using IoT, and benefit from appropriate collaboration among smart IoT devices with mobile agents, illustrated with smart cupboards aimed at tracking memory losses.

The remainder of this paper is organized as follows. The next section introduces the most relevant related work highlighting the gap of the literature covered by the current work. Section III presents a process for improving quality of experience (QoE) of IoT services by means of collaboration of smart devices. Section IV presents a case study for illustrating the proposed process, showing the resulting app and the smart cupboard as work products. Section V shows the experimentation with users about this approach. Finally, section VI mentions the conclusions and future research lines.

II. RELATED WORK

In the literature, several works have addressed the collaboration of IoT smart devices. For example, [5] analyzed the communication network standards in relation to the collaboration of IoT devices, for improving the Quality of Service (QoS) of IoT services. They analyzed the modus operandi of smart objects in IoT ecosystems, and observed a high variety. They proposed some QoS requirements to achieve collaboration in IoT ecosystems. In addition, [6] highlighted the importance of collection of data in IoT systems for collaboration. In particular, they proposed a mechanism for collecting data from IoT devices without a trusted authority, keeping the individual data but preserving their privacy, by ensuring that the source IoT devices are unknown by the data collector when receiving groups of data.

Moreover, [7] is the most relevant work concerning mobile agents for the integration of IoT. This work focuses on how to implement the migration of mobile agents in IoT and the scalability of their approach. Their approach proposed to use standard interfaces for allowing integration among different IoT device types. However, they illustrated their approach with smartphones rather exemplifying their approach with different collaborative IoT smart objects, as the current work does with smart cupboard prototypes.

Several research lines aim at improving QoE in IoT-based services. For example, a research line focuses on providing an

easy and flexible way of interconnecting IoT devices. In this line, [8] presented a service architecture for IoT interoperability, and this architecture is based on a semantic gateway for a standardized interchange of data.

The goal of another research line is to improve the efficiency and scalability of IoT service. Reference [9] proposed to improve the performance and scalability of IoT services by interchanging information among IoT devices by means of cloud computing. Their solution used the novel PaaS framework that facilitated the development of efficient IoT-based systems for providing domain-specific services.

Another line of works dealt with situation-awareness in IoT services. [10] introduced an IoT service platform for coordinating IoT services. This platform was based on the event-driven service-oriented architecture (SOA) paradigm. This work presented a situational event definition language (SEDL) for defining the situational information of IoT devices. They proposed an algorithm for coordinating situational event-driven services.

Moreover, [11] presented the installation of IoT services in the Santander city. They mentioned that the involvement of end users was useful for configuring appropriate testbeds for evaluating IoT services. In addition, Compose [12] is a framework for composing mobile applications that apply cloud computing for managing IoT technology.

Furthermore, [13] developed a web in order to assess users' experience (UX) of home appliances. The web provided 109 questionnaire items related to design elements and UX design principles. They expected that proposed system to be useful for designer of home appliance enterprises, especially for enterprises that were not able to hire UX experts. Finally, the authors highlighted the importance of UX in nowadays; actually they mentioned that one of the well-known strategies for achieving competitive edge in market was to provide superior UX by exploiting Information Technology (IT), the Internet of Things (IoT), and Artificial Intelligence (AI).

In the context of gamification, [14] proposed a technique to include UX principles in design of serious games. They introduced the main components of UX, and proposed a guideline for healthcare games and applications. They conducted a review of Medulla, a serious game in order to explain brain structure and their function. At this review, the authors explained how to perform a design keeping UX design strategies in mind.

Nevertheless, none of these works proposed user-centered design of mobile applications with gamification for actually improving the QoE of end-users in learning the activities related to IoT and improving the collaboration among IoT devices.

III. TECHNIQUE FOR PROVIDING SERVICES WITH COLLABORATION OF IoT

This work proposes to achieve collaboration of IoT by a distributed coordination protocol among IoT devices for achieving multi-configurable services. In particular, it is based on the principles of edge computing but with transferable

software following the paradigm of mobile agents from MASs domain. In the proposed approach, each IoT device provides the service of performing certain software-based filtering and transmission of data from trusted sources. In this way, if an IoT device receives the request with certain software, it starts executing this software for filtering and sending some summarized information to certain IoT device acting as service manager (also referred as main host from this point forward). In a high-level conceptualization, when an engineer wants to install a new IoT service, it installs the software of a MAS in one IoT device. This MAS has the possibility of sending their mobile agents to different IoT devices. These mobile agents are implemented with this transferable software able to be executed in certain IoT device types. These mobile agents apply filtering in different IoT devices, sending only the relevant information back to the main MAS host. This IoT device host collects this relevant information and provides the service to the user based on the collaboration of all the IoT devices achieved by a MAS with mobile agents.

This proposed mechanism is illustrated with the activity diagram of Figure 1. Notice that this figure uses different background colors for distinguishing whether activities are performed by the main host IoT device (in green) or other IoT devices (in blue). Notice that this diagram only provides full details for one non-main collaborative IoT device, and all the others (up to any number) use the same flow of activities, so these flows are omitted for avoiding repetition in the diagram. Notice that each IoT device is executed in parallel, and uses edge computing by performing most computational tasks in the edge (i.e. each IoT device). Only the summarized relevant information is sent to the main host as commonly done in edge computing. By relevant, we mean only the minimum necessary information so the global processing can be performed. Regarding the activity of providing type of sensorized data, the IoT device can send different types such as accelerometer data, door states (i.e. open/closed), detection of human presence in a given spot, temperature and images/videos taken from a camera. In this collaborative environment, the transference of agent data involves to send the agent source code as well as its attribute values, so the agent can continue its execution in a different IoT device, allowed and assisted by the corresponding host device.

In order to guarantee security in IoT services in the production stage, we recommend that IoT devices use anti-virus software to analyze the code of the received mobile agents for avoiding executing malware. In addition, the permissions of mobile agents should be limited to prevent certain kinds of attacks such as the ones that involve rewriting the code of the host device. In addition, this approach can apply the common adaptive trust and reputation models about mobile agents from the literature [15].

We also propose to improve UX in IoT services by developing ad-hoc 3D instructional games for the installation of collaborative IoT services. Figure 2 presents the proposed process of the current approach. Developers can follow this process to obtain a mobile application specifically designed

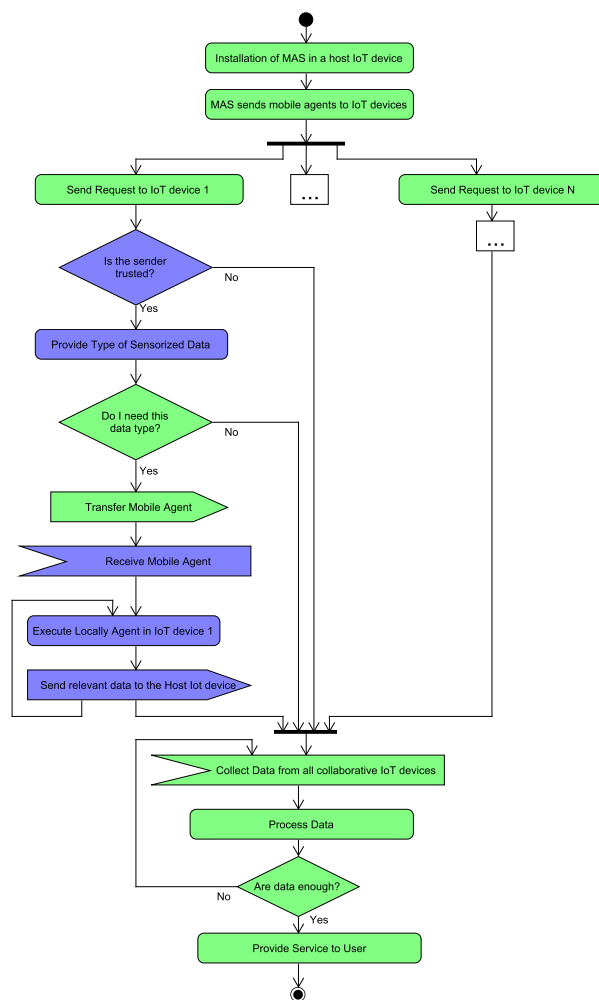


FIGURE 1. Mechanism for collaboration of IoT with mobile agents executed in the edge.

for guiding user in using an IoT service. This process is based on a user-centered design. The first part of the process is focused on both (a) designing an easy-to-use IoT service and (b) determining the learning objects as the most relevant aspects that users need to know for using the IoT service.

The goal of second part of the process is to design and develop the game that guarantees that the user learns every learning object when completing the game. This process part incorporates the testing with the users, and the integration of their feedback into the game-based app. After including the feedback of each user, they test the app again until they are completely satisfied.

This process may generally improve the UX in IoT services, since users can generally like to learn the difficult parts of the IoT services by game application.

This process recommends to use Unity 3D for developing this kind of game, as commonly done in instructional game-based applications [16]. Since Unity 3D is a multi-platform

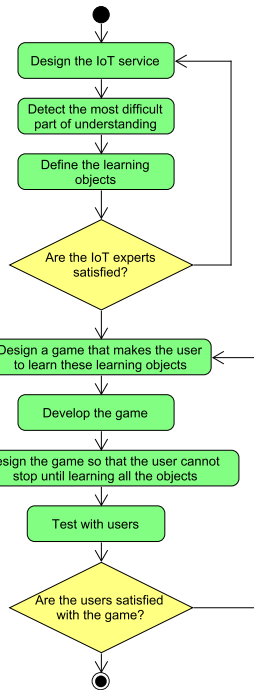


FIGURE 2. Process for developing tailored mobile applications for guiding people in learning to use collaborative IoT services.

environment, the apps can be compiled for different platforms such as Android and iOS.

Since in this generic process the IoT services can be very different from each other, some restrictions and details must be concreted for each IoT service. This work recommends developers to indicate the most relevant agreements after each activity of the presented process. The next section presents a case study of applying this process, indicating the agreements for each activity

IV. CASE STUDY ABOUT COLLABORATIVE IoT SMART CUPBOARDS

In order to exemplify the current approach, we built a prototype of collaborative smart cupboards that can apply the current approach. All the smart cupboards have initially the same software that can act as both as main host IoT device of a service or as collaborative IoT device for providing information to another host. Each smart cupboard can execute a mobile agent for the filtering of data from their door sensors, if any mobile agent is hosted. Each smart cupboard can also execute a MAS that distributes mobile agents. Potentially this approach could be executed in any number of smart cupboard with different distributions in a kitchen, and consequently this approach could be potentially deployed in any kitchen.

We designed this smart cupboard as part of an AAL project focused on detecting and tracking the symptoms of Alzheimer's disease (AD) patients. Figure 3 shows a prototype of this smart cupboard. This cupboard has sensors that track whether the doors are opened or closed. Their purpose is to assess whether the user opens the door more times than

necessary, by looking many times in different doors of the same cupboard like looking for something that they forgot where they have placed it.

In the design of an IoT service that tracks health indicators, we selected an object commonly used daily by people that it could track memory losses, which is one of the main symptoms of AD. We decided that a kitchen cupboard is common in most houses, and people use it on a daily basis, since they usually need food stored in these cupboards for cooking their meals.

As people with memory losses usually forget whether they have placed certain items, we assumed that they could also forget whether they have placed the different food kinds in a cupboard. When a person has forgotten where some food is, they would normally check different cupboard doors checking one after other very fast. Thus, we decided to monitor the opening/closing of each door.

For this purpose, we installed door sensors in the cupboard connected to a Raspberry PI 3 also attached to the cupboard. This Raspberry is connected to power electricity, and connects to Internet via WiFi. Figure 4 shows this part of the smart cupboard.

The Raspberry collects the changes of states of the door sensors from closed to open from the different doors. Normally, a person that properly remembers where the food is just opens the doors they need and these openings are separated in time. However, when people are looking for something, they normally repeatedly open the doors until they find what they need. A simple program can detect this pattern and allow users to access a basic evaluation of their memory capabilities based on whether these patterns have been detected.

In this smart cupboard, we have detected two aspects in which users may find difficulties. First, as a low-cost solution, familiars and caregivers would need to install the door sensors and the Raspberry PI with the appropriate software on their cupboards. An app could be useful for teaching this installation process. Second, another app could be useful for instructing users in performing certain steps for the calibration of the smart cupboard with a game-like approach, where users can play to remind items in the cupboard and try to find these by opening the appropriate cupboard doors. In this case, the user would be instructed to place certain food kinds in the cupboard, and the app then would challenge them in finding certain food kinds in the cupboard.

Smart cupboard prototype is formed, with regard to hardware, by a Raspberry Pi (RP) 3 B+, a protoboard, several jumper wires and a door sensor. RP owns CPU of 1.4 GHz 64-bit quad-core ARM v8, 1 GB RAM, 4 USB ports, inputs and outputs video and audio, although we have to highlight their GPIO Header (General Purpose Input/Output). The RP owns 20 couples of pins in order to several reasons; in our case, we have used these pins in order to connect the RP and the sensor door. The door sensor only needed two connections, one of them was to a pin ground and the remaining one was to a pin available to user. 24 pins of the 40 of RP were available in order to let the user use them as they wanted.



FIGURE 3. A prototype of a collaborative IoT smart cupboard.

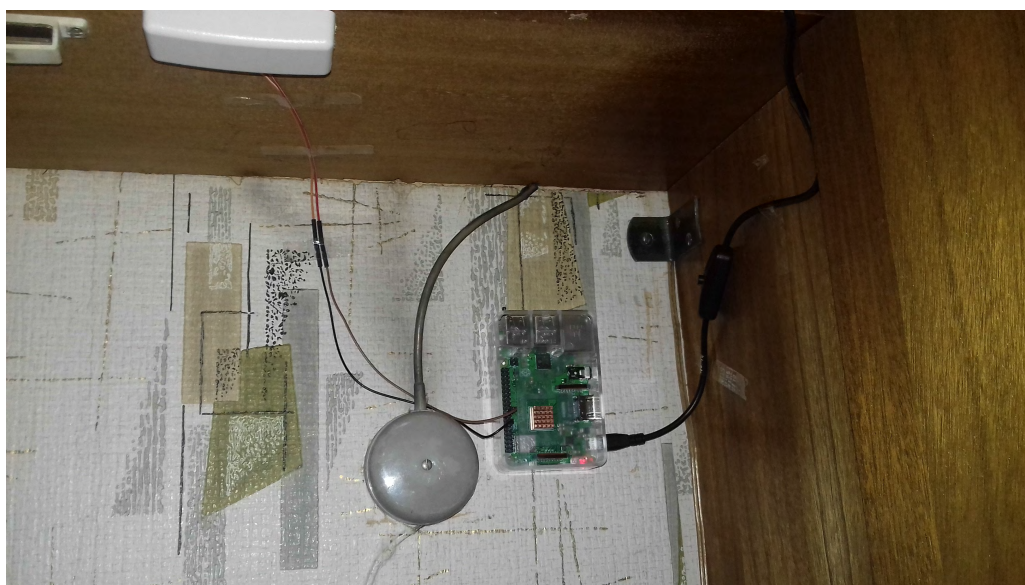


FIGURE 4. The Raspberry connected to the door sensor in the smart cupboard prototype.

In this prototype, to avoid weld electronic components we have used a protoboard in order to connect door sensor to RP by means of jumper wires. RP and other components were fitted inside of cupboard with adhesive tape and screws. Door sensor was composed of two parts, one of them was at top of cupboard and the other part was pasted to door, in ways that when cupboard has the door close, two parts of sensor matched allowing close a circuit and emitting a type of signal. Conversely, when a door was opened, the circuit was interrupted and other type of signal was emitted.

Regarding to software, we have developed a script written in Python programming language in order to receive door

sensor signals and management it. On the script, we have imported GPIO library in order to receive signals from pins. Therefore, we had to keep several features in mind; the first was to establish which of two numeration systems of pins were going to be used, which were BCM and BOARD. In BOARD system, the numeration of pins was based in the physical order of pins on board, it meant from 1 to 40. The BCM system used a certain number of GPIO proposed by RP documentation, this last system was used at our script. Other thing to keep in mind was to set up a certain pin as input pin, logically the chosen pin was the pin that allowed to connect RP and the door sensor. Finally, through an infinite

loop, the system kept listening any change in door sensor; if the door of smart cupboard was opened or closed, the infinite loop managed a certain signal and performed consequently.

The tracking of memory losses and the notification to the user is performed following the dataflow diagram of Figure 5. Our system is always in execution, due to this fact, the sensors are always to await who anybody open the door. When a user opens the door, the system immediately saves the date and hour of this event. The saved time is obtained in order to

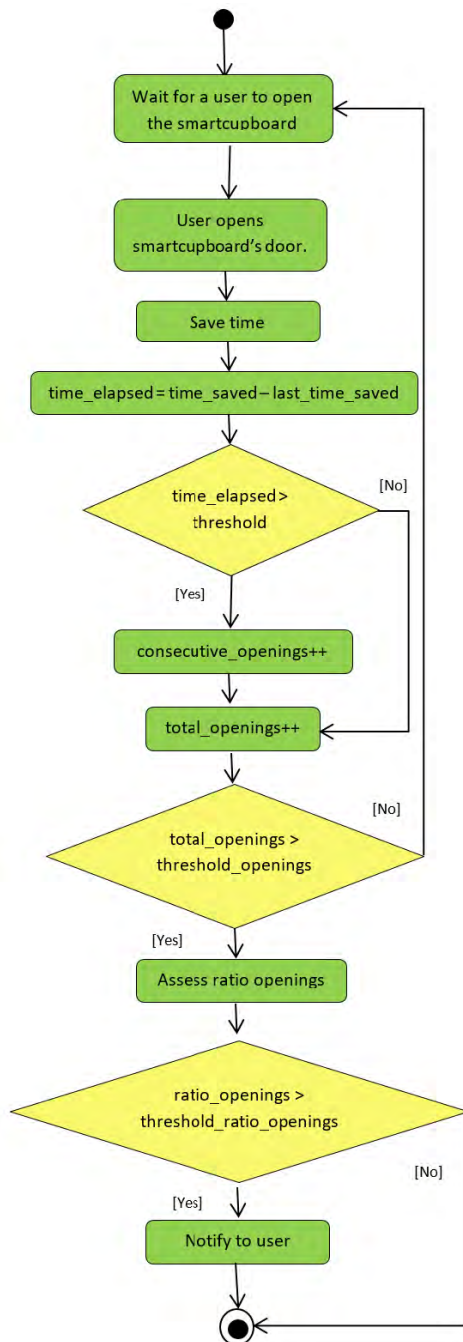


FIGURE 5. Dataflow diagram for tracking memory losses in users by means of the smart cupboard.

calculate the elapsed time from the last time a user opened the door of smart cupboard. If the elapsed time is below a certain threshold, the system increases the consecutive opening counter. Independently of elapsed time, the system always adds a unit to the total opening counter. These counters allow the program to calculate the ratio opening of user, whose function aims at determining whether this user has a common symptom of AD. Once total opening counter is increased, the threshold opening is assessed, this threshold indicates which is minimum times that a user needs to open the door to carry out ratio a memory assessment, i.e. if threshold opening is 100, this mean that each 100 times that user opens the door of smart cupboard, it diagnoses whether user could have AD symptoms. In case there are symptoms, the user is notified. Otherwise, threshold opening is rebooted and the system keeps going on. This initial smart cupboard prototype provides feedback through the screen of laptop so the user can read messages. However, we are considering other ways such as a text message to mobile phone or device, develop an application that can receive alerts, website, or maybe we could add to smart cupboard a LCD screen so users could read messages. In order to instruct the mechanism of learning in IoT devices with a game-base app, we used a prototype app for the experiments.

V. EXPERIMENTATION

A. PARTICIPANTS

We recruited 20 people for participating in this user study. They were 27.85 years old in average (SD = 5.66) and studied 15.65 years in average (SD = 3.54). Among the participants, only 30% were studying or working in computer science field. 65% of participants were male. Participants did the test voluntarily without getting paid. Participants were familiar with mobile devices, and did not have any experience with meditation poses.

B. PROCEDURE

In this experimentation, we followed the same procedure with each participant. The experimenter introduced the IoT to each participant through a briefly explication about these topics. The experimenter introduced the presented prototypes to the user. The experimenter told each participant that two learning objects would appear on the application and they will have 10 seconds for memorizing each of them. In order to avoid the influence of the learning effect among between different learning objects with images, we counterbalanced the order of experimenting these. Once a participant has memorized an image, the experimenter asked them to replicate this with the app by controlling an avatar. Since one of the goals of this study was to assess the usability, the experimenter did not provide any instruction about how to control the avatar, avoiding mentioning words such as “touch”, “drag”, “hold” and “finger”. Conversely, the phrase for asking the user to use the app to replicate the posture was literally “Please, now replicate this image with the application”. Our hypothesis

TABLE 1. Questionnaire for evaluating the proposed Service-centric IoT approach.

ID	Question
1	Do you think this app has successfully helped you in learning the use of this IoT system?
2	Do you think that a similar app could assist you in properly placing sensors for an IoT system?
3	Do you think a similar app could help you in understanding several IoT-related domains such as smart memory assessment and body sensor networks?
4	Do you think an app similar to this could help you in adapting a house into a smart house (e.g. by watching a video of a person installing the devices and then practicing this installation with an avatar)?
5	How much do you think an app like this could help you in understanding the use of IoT (e.g. by practicing the interactions with a smart home through an avatar)?

was that if the application was sufficiently easy to use and intuitive, they would have no problem in learning how to use it and using it.

The experimenter asked each participant to retry each learning object until representing it successfully. The app gave feedback by hints so the user knows what aspects were wrong in the response.

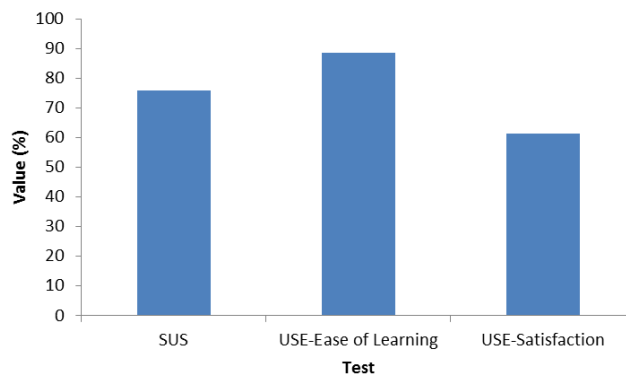
We repeated this task of successfully representing both poses three times with each participant, referring to the representation of each learning object as tests 1 to 6 in chronological order.

During the test, we measured the reaction time and the number of trials for successfully representing each image. Finally, after the task ended, each participant was asked to reply the validated System Usability Scale (SUS) [17] scale and the ease of learning and satisfaction dimensions of Usefulness, Satisfaction, and Ease of use questionnaire (USE) [18]. In addition, the experimenter asked a questionnaire about our IoT approach. We defined the questions of this questionnaire for this experimentation. Table 1 shows the questions, and these are replied in a seven-point Likert scale from not at all (1) to very much (7).

Moreover, we measured the performance of the system by measuring the update response time per frame. These measures focused on the inverse kinematics calculation and its rendering. We also measured the time that the system took for the automatic pose classification. We also measured the memory resources used by the system.

C. RESULTS AND DISCUSSIONS

All the participants successfully completed the tasks of this experiment. Figure 6 shows the average results of SUS and USE tests. The exact value of SUS test was 75.75% in average. This result revealed the high usability of the app, and consequently the app was probably properly designed from a usability viewpoint. In addition, the experimenter appreciated that none of the participants had problem in deducing how to use their own finger to drag the parts of the avatar. Maybe, users without enough patience or without continuous contact

**FIGURE 6.** Results of USE and SUS tests.

with mobile devices did not consider the application ease-of-use, and due to this fact we did not obtain higher results in SUS test.

Regarding to USE test, from its four independently validated dimensions, we only used the dimensions of ease of learning and satisfaction. The mean result of USE-Ease of learning test was 88.54%. Thus, the app and the smart IoT object were easy to learn according to this validated scale. Regarding the exact value of USE-Satisfaction was 61.43% on average. This dimension was the least ranked probably because most participants were not interested in meditation poses.

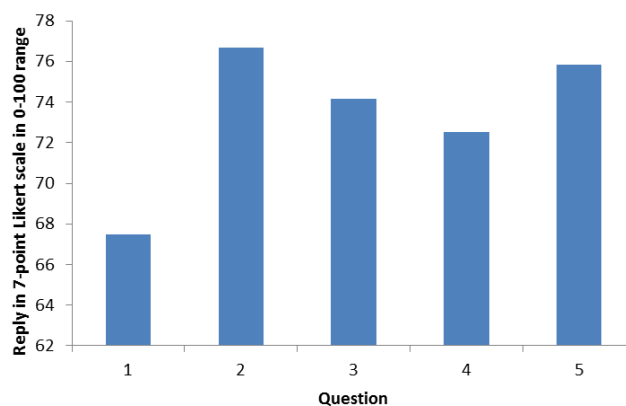
**FIGURE 7.** Results of the questionnaire designed for the proposed service-centric IoT approach.

Figure 7 shows the average result for each question of our service-centric IoT test. It is worth highlighting that all questions obtained a rank above 65%. Thus, all research utilities of the current approach can be considered as promising. The first question obtained 67.5% on average (SD = 1.46), and all the other values obtained results of 72.50% or above. This lower value on the first question may be explained because participants were not familiarized with this kind of IoT learning objects, and consequently may not understood the relevance of meditation compared to other research lines. Considering all the results, we can conclude that participants thought that this type of application could be used for different purposes

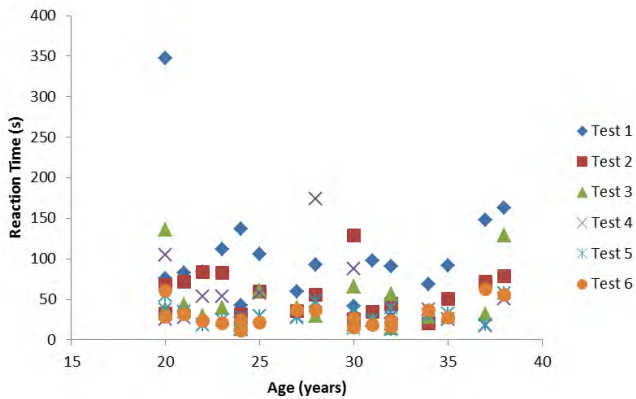


FIGURE 8. Comparison of reaction times between tests 1 to 6 considering age.

in the context of service-centric IoT. Since these questions considered IoT topic, the results advocate that the proposed approach may be suitable for introducing IoT objects to users. The second question is highlighted because it had the highest score, concretely 76.67% in average (SD = 1.39). Thus, a high amount of users considered that the proposed approach could be useful for instructing users in placing sensors for an IoT system.

Figure 8 exposes a dispersion graph about the relation of reaction time and age comparing the results of tests 1 to 6. The reader can notice that for each participant the first test generally took more time than the other tests. This fact advocates that the app was useful for learning similar IoT objects, since after representing one learning object the user improved the time for successfully adopting the same learning object or a similar one. In order to further assess this fact, we performed the paired t-test statistical test between the reaction times of each pair of consecutive tests using the data from all the participants. Figure 9 presents the results of these paired t-test. The differences between tests 1 and 2 were significant with a significance level of 0.015 and a t statistic of 2.609. Most of other pairs of consecutive tests were non-significant except between tests 4 and 5. The reason might be that with four tests, the effects of learning the app and the specific posture are shown together. In the statistics related with these

paired t-tests in Figure 10, one can observe that between the test 1 and test 2, the average time decreased from 96.50 s to 54.20 s. The reduction between test 4 and test 5 was from 45.90 s to 29.75 s.

The reader can also notice that reaction time was slightly dependent on age because the difference between participants with 35 - 40 years old and the other ones was not very different. Perhaps, if we had participants with range between 40 - 60 years old, the difference would be more notorious. At this point, we can affirm that at a higher age of the user the reaction time was slightly greater. In order to statistically assess whether this relation was significant, we conducted two different correlation tests, considering the results of the last user test. Figure 11 presents the results of the Pearson correlation test, and Figure 12 indicates the results of Spearman's Rho. Both correlation tests did not detect any significant correlation. Although memory is usually related age, this experiment may not have a sample enough large to detect this correlation as significant.

Figure 13 exposes another dispersion graph that relates reaction time and the number of education years of each participant. One can observe an outlier case with 350 s, but others had certain regularity. By observation, we did not appreciate any pattern, and consequently we cannot affirm that reaction time was dependent on participant's education. Notice that all people of the sample were used to mobile devices regardless their number of education years.

Figure 14 exposes a dispersion graph that compares the number of trials for successfully representing each pose between tests 1 to 6, considering age. In this graph, one can observe that the most results were in range 1-2 trials. Nevertheless, we can highlight users between 35 - 40 years old generally needed 2 trials or more. This fact shows a possible direct dependency between number of trials and age, in which the older a person is, usually the greater number of trials is.

Moreover, we performed paired t-tests to evaluate the learning process with this app by comparing the number of trials from each pair of consecutive tests in tests 1 to 6. Figure 15 shows the results of the paired t-test. In this case, the difference between tests 1 and 2 was significant with a significance level of 0.016, while all the other consecutive

Paired Samples Test

		Mean	Std. Deviation	Paired Differences		t	df	Sig. (2-tailed)
				Std. Error Mean	95% Confidence Interval of the Difference			
				Lower	Upper			
Pair 1	RT Test 1 - RT Test 2	42,300	70,331	15,726	9,384 75,216	2,690	19	,015
Pair 2	RT Test 2 - RT Test 3	9,900	37,922	8,480	-7,848 27,648	1,167	19	,257
Pair 3	RT Test 3 - RT Test 4	-1,600	43,799	9,794	-22,099 18,899	-,163	19	,872
Pair 4	RT Test 4 - RT Test 5	16,150	32,214	7,203	1,074 31,226	2,242	19	,037
Pair 5	RT Test 5 - RT Test 6	-,250	12,174	2,722	-5,947 5,447	-,092	19	,928

FIGURE 9. Paired t-test results about reaction times in consecutive user tests.

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	RT Test 1	96,50	20	70,469	15,757
	RT Test 2	54,20	20	26,948	6,026
Pair 2	RT Test 2	54,20	20	26,948	6,026
	RT Test 3	44,30	20	33,298	7,446
Pair 3	RT Test 3	44,30	20	33,298	7,446
	RT Test 4	45,90	20	38,145	8,529
Pair 4	RT Test 4	45,90	20	38,145	8,529
	RT Test 5	29,75	20	13,392	2,995
Pair 5	RT Test 5	29,75	20	13,392	2,995
	RT Test 6	30,00	20	14,924	3,337

FIGURE 10. Statistics of reaction times about the paired t-test.

		Age	RT Test 2
Age	Pearson Correlation	1	,016
	Sig. (2-tailed)		,945
	N	20	20
RT Test 2	Pearson Correlation	,016	1
	Sig. (2-tailed)	,945	
	N	20	20

FIGURE 11. Pearson test about the correlation of reaction time and age.

pairs were no significant. Figure 16 shows that number of trials decreased from 2.85 to 1.75 from test 1 to test 2. This reveals that the user probably significantly learned the objects and to represent these in the first test.

Figure 17 shows another dispersion graph that relates the number of trials with the number of education years. In a similar way to the aforementioned case, the number of trials ranged between 1 and 2 trials, but in this case the relation was clearer than in the previous case. The reader can notice that the number of trials usually decreased when the education increased. In other words, users with higher levels of study were more familiarized with being evaluated and probably learned better from the constructive feedback. Hence, people with low levels of education may need more trials for learning from this type of applications.

Up to this point, a feature common among all dispersion graphs is the progressive learning of all participants. The reaction time and number of trials were significantly reduced from the first pose representation to the next one. The reaction time and the number of trials were generally lower in each test, and consequently most people used to mobile devices will probably be able to adequately use the current app and similar ones without almost any problem.

Figure 18 exposes the system computing response time for updating the 3D virtual avatar representation for each frame. Concretely, we have measured the time that the app needed

		Age	RT Test 2
Spearman's rho	Age	Correlation Coefficient	1,000
		Sig. (2-tailed)	,837
		N	20
RT Test 2	Age	Correlation Coefficient	-,049
		Sig. (2-tailed)	,837
		N	20

FIGURE 12. Spearman's rho about the correlation of reaction time and age.

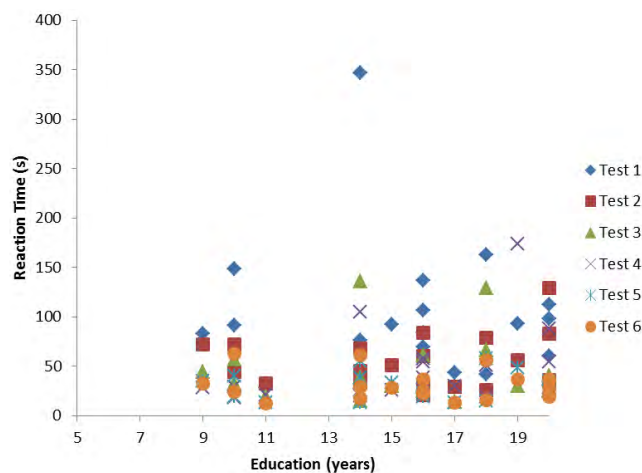


FIGURE 13. Reaction time considering the number of education years.

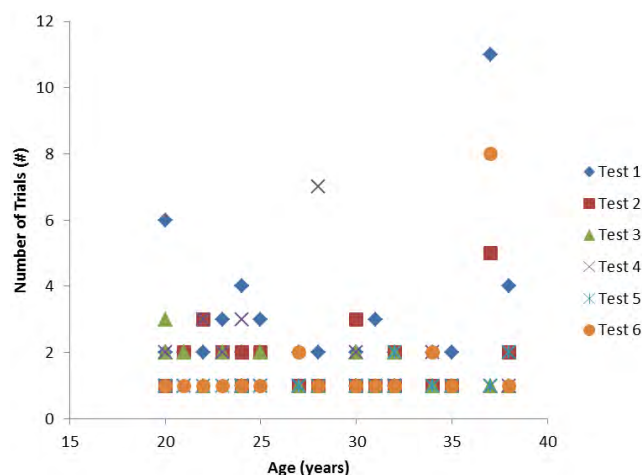


FIGURE 14. Comparison of number of trials for tests 1 to 6, considering age.

to recalculate avatar's position and rendering it. Since the avatar's body parts were connected through joints, when the user dragged a body part, then some of the other body parts also moved like in real life. The app achieved this natural movement by means of inverse kinematics. The system response time was measured while a participant was trying to represent a learning object. The time was measured 1300 times. The reader can notice that in most cases this time

Paired Samples Test

		Paired Differences							
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference		t	df	Sig. (2-tailed)
					Lower	Upper			
Pair 1	NT Test 1 - NT Test 2	1,100	1,861	,416	,229	1,971	2,643	19	,016
Pair 2	NT Test 2 - NT Test 3	,350	1,309	,293	-,263	,963	1,196	19	,246
Pair 3	NT Test 3 - NT Test 4	-,300	1,625	,363	-1,061	,461	-,825	19	,419
Pair 4	NT Test 4 - NT Test 5	,600	1,501	,336	-,102	1,302	1,788	19	,090
Pair 5	NT Test 5 - NT Test 6	-,350	1,631	,365	-1,113	,413	-,960	19	,349

FIGURE 15. Paired t-test for comparing the number of trials between consecutive pairs in tests 1 to 6.

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	NT Test 1	2,85	20	2,254	,504
	NT Test 2	1,75	20	1,020	,228
Pair 2	NT Test 2	1,75	20	1,020	,228
	NT Test 3	1,40	20	,598	,134
Pair 3	NT Test 3	1,40	20	,598	,134
	NT Test 4	1,70	20	1,418	,317
Pair 4	NT Test 4	1,70	20	1,418	,317
	NT Test 5	1,10	20	,308	,069
Pair 5	NT Test 5	1,10	20	,308	,069
	NT Test 6	1,45	20	1,572	,352

FIGURE 16. Statistics about paired t-test concerning number of trials.

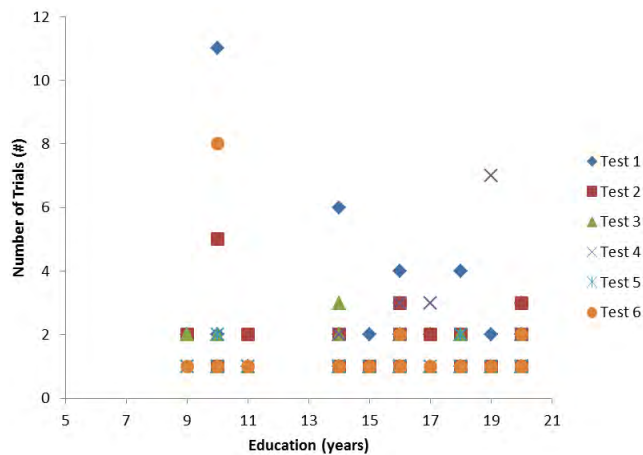


FIGURE 17. Number of trials vs education.

was not greater than 0.0001 s. These time periods matched with the moments in which the participant was either not doing anything or thinking about what part to move. Certain peaks appeared in the graph and they matched with the moments that the participant was moving certain joint. In this time periods, the app was calculating each angle, torque and orientation of selected joint and at the same was calculating inverse kinematics for all the other connected body parts. For instance, when the participant moved one of the avatar's part,

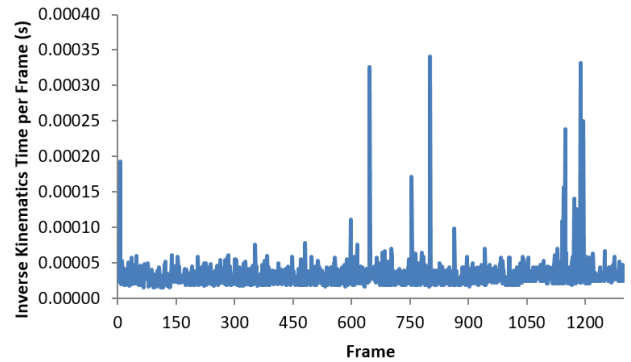


FIGURE 18. Performance about avatar's position.

the app calculated the aforementioned parameters for the corresponding part and other connected joints such as the knee. Finally, our avatar did not have constraints on their joints. On the one hand, the amount of operations was lesser so operation time was also lower. On the other hand, the avatar was able to adopt very hard and unnatural postures, such as the ones in which both feet were above their head. In summary, the system response times were low enough so users could perceive the drag-and-drop operations as real-time.

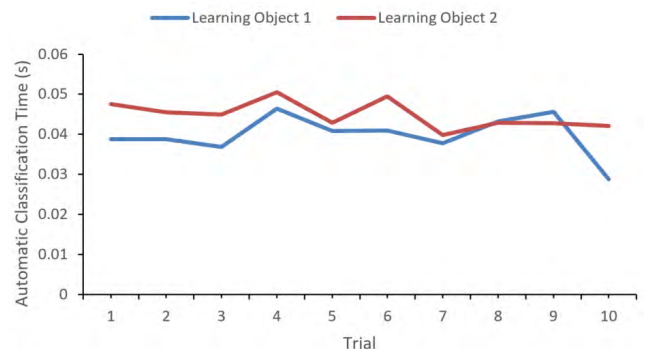


FIGURE 19. Performance of the automatic classification of the system.

Figure 19 depicts the times that the system needed to determine whether an avatar's posture was correct. This operation needed to perform certain classification tasks over certain

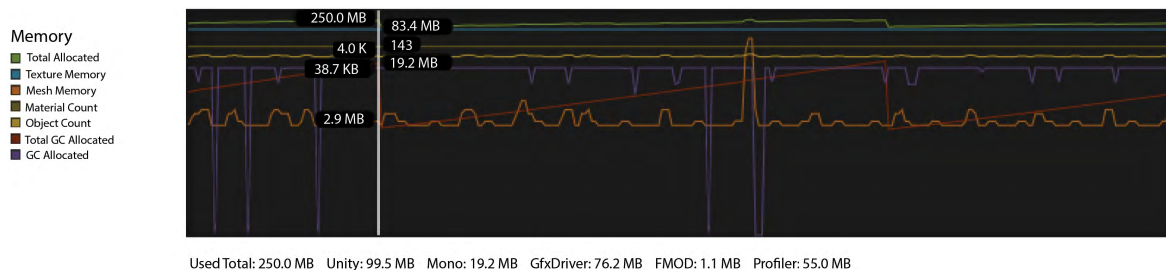


FIGURE 20. Evaluation of RAM memory usage with unity profiler tool.

aspects of the learning object. We decided to analyze this time since this operation had one of the highest computational costs. Once the user pressed the 'done' button, the app evaluated the posture. This operation was more or lesser costly regarding the joint positions. We have obtained this graph by means of several trials. We performed 20 trials, 10 with one learning object and 10 with another. Each try was random, meaning that in each trial the avatar could be with all their extremities crossed among them or even the avatar could be well positioned. Regardless the posture, the classification time was always measured. Most of the results were in the range between 0.03 and 0.05 s, with an average of 0.0423 s (SD = 0.0049). Like in the previous case, we consider this response time as appropriate, because it was lower than the common minimum time noticeable by humans (i.e. 0.2 s). This graph shows that there were no big differences between the two learning objects, although one of them needed slightly lower time in most cases.

Since the app was made with Unity, we used its common performance-evaluation tool. Specifically, its embedded Profiler tool showed the amount of used RAM memory. Figure 20 shows the used RAM memory during a normal use of the application. The reader can notice that the total used memory (top green line) was cyclical or their behavior had a recursive pattern, and the total memory did not exceed 250 MB. We highlight that RAM memory was used to calculate operations, save textures and so on. Positions of mesh's vertex, color of each triangle of avatar or texturing mapping was duty of graphic card, and the management of these resources depended on the graphic card type. Since common devices has greater RAM storage (e.g. between 1.5 GB and 16 GB), we consider this result as promising because the app could be executed in most actual devices.

VI. CONCLUSION

This article has proposed a technique for providing collaboration of IoT devices. This technique has been illustrated with the development of collaborative smart cupboards connected to Internet. A user study revealed the potential of this approach for improving the QoE of IoT-based services. The users reported high levels of usability, ease of learning and satisfaction with this approach. An ad-hoc questionnaire showed that users thought that the proposed approach could

be useful in different contexts of IoT services. The performance of the system was appropriate for the continuous calculations, rendering per frame and classification in terms of response times. The usage of RAM memory was also adequate considering the common actual devices.

In the future, we plan to design a more complete and elaborated AAL system for assisting AD carriers, integrating the smart cupboard with other smart objects of different types. The AAL system will be deployed by installing a kit of low-cost IoT devices. We will develop an instructional app following the proposed approach to guide caregivers and familiars in installing and using the IoT smart objects of the AAL system.

ACKNOWLEDGMENT

This work was mainly performed during the research stay of the first author in the Massachusetts General Hospital and Harvard University.

REFERENCES

- [1] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.
- [2] I. García-Magariño, S. Sendra, R. Lacuesta, and J. Lloret, "Security in vehicles with IoT by prioritization rules, vehicle certificates and trust management," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2871255.
- [3] I. García-Magariño, G. Palacios-Navarro, R. Lacuesta, and J. Lloret, "ABSCEV: An agent-based simulation framework about smart transportation for reducing waiting times in charging electric vehicles," *Comput. Netw.*, vol. 138, pp. 119–135, Jun. 2018.
- [4] F. González-Landero, I. García-Magariño, R. Lacuesta, and J. Lloret, "Green communication for tracking heart rate with smartbands," *Sensors*, vol. 18, no. 8, p. 2652, 2018.
- [5] O. Bello and S. Zeadally, "Toward efficient smartification of the Internet of Things (IoT) services," *Future Gener. Comput. Syst.*, vol. 92, pp. 663–673, Mar. 2019.
- [6] Y.-N. Liu, Y.-P. Wang, X.-F. Wang, Z. Xia, and J.-F. Xu, "Privacy-preserving raw data collection without a trusted authority for IoT," *Comput. Netw.*, to be published, doi: 10.1016/j.comnet.2018.11.028.
- [7] T. Leppänen *et al.*, "Mobile agents for integration of Internet of Things and wireless sensor networks," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Oct. 2013, pp. 14–21.
- [8] P. Desai, A. Sheth, and P. Anantharam, "Semantic gateway as a service architecture for IoT interoperability," in *Proc. IEEE Int. Conf. Mobile Services (MS)*, New York, NY, USA, Jun./Jul. 2015, pp. 313–319.
- [9] F. Li, M. Vögler, M. Claeßens, and S. Dustdar, "Efficient and scalable IoT service delivery on cloud," in *Proc. IEEE 6th Int. Conf. Cloud Comput. (CLOUD)*, Santa Clara, CA, USA, Jun./Jul. 2013, pp. 740–747.
- [10] B. Cheng, D. Zhu, S. Zhao, and J. Chen, "Situation-aware IoT service coordination using the event-driven SOA paradigm," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 2, pp. 349–361, Jun. 2016.
- [11] L. Sanchez *et al.*, "SmartSantander: IoT experimentation over a smart city testbed," *Comput. Netw.*, vol. 61, pp. 217–238, Mar. 2014.

- [12] C. Doukas and F. Antonelli, "COMPOSE: Building smart & context-aware mobile applications utilizing IoT technologies," in *Proc. Global Inf. Infrastruct. Symp.*, Trento, Italy, Oct. 2013, pp. 1–6.
- [13] J. Park et al., "Development of a Web-based user experience evaluation system for home appliances," *Int. J. Ind. Ergonom.*, vol. 67, pp. 216–228, Sep. 2018.
- [14] J. R. Fanfarelli, R. McDaniel, and C. Crossley, "Adapting UX to the design of healthcare games and applications," *Entertainment Comput.*, vol. 28, pp. 21–31, Dec. 2018.
- [15] D. Shehada, C. Y. Yeun, M. J. Zemerly, M. Al-Qutayri, Y. Al-Hammadi, and J. Hu, "A new adaptive trust and reputation model for mobile agent systems," *J. Netw. Comput. Appl.*, vol. 124, pp. 33–43, Dec. 2018.
- [16] L. Chittaro, "Designing serious games for safety education: 'Learn to Brace' versus traditional pictorials for aircraft passengers," *IEEE Trans. Vis. Comput. Graphics*, vol. 22, no. 5, pp. 1527–1539, May 2016.
- [17] J. Brooke, "SUS-A quick and dirty usability scale," *Usability Eval. Ind.*, vol. 189, no. 194, pp. 4–7, 1996.
- [18] A. M. Lund, "Measuring usability with the use questionnaire¹²," *Usability Interface*, vol. 8, no. 2, pp. 3–6, 2001.

Authors' photographs and biographies not available at the time of publication.

•••

6.2. Smart cupboard for assessing memory in home environment.

Cita completa:

GONZÁLEZ-LANDERO, F., GARCÍA-MAGARIÑO, I., AMARIGLIO, R., & LACUESTA, R. (2019). Smart cupboard for assessing memory in home environment. *Sensors*, 19(11), 2552.

Abstract:

Sensor systems for the Internet of Things (IoT) make it possible to continuously monitor people, gathering information without any extra effort from them. Thus, the IoT can be very helpful in the context of early disease detection, which can improve peoples' quality of life by applying the right treatment and measures at an early stage. This paper presents a new use of IoT sensor systems. We present a novel three-door smart cupboard that can measure the memory of a user, aiming at detecting potential memory losses. The smart cupboard has three sensors connected to a Raspberry Pi, whose aim is to detect which doors are opened. Inside of the Raspberry Pi, a Python script detects the openings of the doors, and classifies the events between attempts of finding something without success and the events of actually finding it, in order to measure the user's memory concerning the objects' locations (among the three compartments of the smart cupboard). The smart cupboard was assessed with 23 different users in a controlled environment. This smart cupboard was powered by an external battery. The memory assessments of the smart cupboard were compared with a validated test of memory assessment about face-name associations and a self-reported test about self-perceived memory. We found a significant correlation between the smart cupboard results and both memory measurement methods. Thus, we conclude that the proposed novel smart cupboard successfully measured memory.

Article

Smart Cupboard for Assessing Memory in Home Environment

Franks González-Landero ¹, Iván García-Magariño ^{2,*}, Rebecca Amariglio ^{3,4} and Raquel Lacuesta ^{5,6}

¹ Edison Desarrollos, 44002 Teruel, Spain; gonzalezfranks@edisondesarrollos.es

² Department of Software Engineering and Artificial Intelligence, Complutense University of Madrid, 28040 Madrid, Spain

³ Harvard Medical School, Harvard University, Boston, MA 02115, USA; ramariglio@mgh.harvard.edu

⁴ Massachusetts General Hospital, Boston, MA 02114, USA

⁵ Department of Computer Science and Engineering of Systems, University of Zaragoza, 44003 Teruel, Spain; lacuesta@unizar.es

⁶ Instituto de Investigación Sanitaria Aragón, University of Zaragoza, 50009 Zaragoza, Spain

* Correspondence: igarciam@ucm.es; Tel.: +34-913-947-643

Received: 26 April 2019; Accepted: 31 May 2019; Published: 4 June 2019



Abstract: Sensor systems for the Internet of Things (IoT) make it possible to continuously monitor people, gathering information without any extra effort from them. Thus, the IoT can be very helpful in the context of early disease detection, which can improve peoples' quality of life by applying the right treatment and measures at an early stage. This paper presents a new use of IoT sensor systems—we present a novel three-door smart cupboard that can measure the memory of a user, aiming at detecting potential memory losses. The smart cupboard has three sensors connected to a Raspberry Pi, whose aim is to detect which doors are opened. Inside of the Raspberry Pi, a Python script detects the openings of the doors, and classifies the events between attempts of finding something without success and the events of actually finding it, in order to measure the user's memory concerning the objects' locations (among the three compartments of the smart cupboard). The smart cupboard was assessed with 23 different users in a controlled environment. This smart cupboard was powered by an external battery. The memory assessments of the smart cupboard were compared with a validated test of memory assessment about face–name associations and a self-reported test about self-perceived memory. We found a significant correlation between the smart cupboard results and both memory measurement methods. Thus, we conclude that the proposed novel smart cupboard successfully measured memory.

Keywords: IoT; memory loss; e-healthcare; Alzheimer's; door sensors

1. Introduction

Dementia is the progressive loss of cognitive functions due to brain damage or disorder. Among dementia types, one of the most well-known and widespread diseases is Alzheimer's disease, and the number of people who will suffer from this disease is estimated to reach 131.5 million by 2050 [1]. This disease hampers daily life activities such as recognizing faces and remembering names, places, and positions [2]. Potentially 131.5 million people could put themselves at risk if they start developing these symptoms without the proper cautionary measures and palliative treatments.

There is no cure for Alzheimer's disease, but there are palliative treatments. Some of these are medicines, but none of them has been proven to stop the progression of this disease [3]. Other examples are psychosocial interventions, and these involve stimulation-oriented treatments with art, music,

animals, or other recreational activities; however, the efficacy of these treatments remains uncertain [4]. The last of the palliative treatments is caregiving, which is probably the safest one, but it has a great impact in health economics for the necessary resources—mainly caregivers, but also measurement of the state of the disease for suitable caregiving, tagging items in houses, and the maintenance of feeding tubes in the case of eating problems.

On the other hand, the literature claims that Alzheimer's disease represents the main cause of neurodegenerative dementia in the population aged over 60 years old, with an estimated prevalence of 5–7% [5]. People increase the probability of starting to suffer from Alzheimer's disease when getting older without noticing. If anyone suffers from Alzheimer's disease, they need to receive some treatment—the sooner the better.

At present, most people live surrounded by technology, including Internet of Things (IoT) sensor objects that can collect, pre-process, and analyze continuous streams of data (e.g., weather, traffic, finance, and health data). One of the most common goals of the IoT is to enhance the quality of life. IoT technology can track the interactions between quotidian objects and persons, or even among objects, contributing to the digitalization of the physical world. Another goal of the IoT is to connect and synchronize traditional utensils through the Internet in order to deliver a service more efficiently. In this way, all elements that used to connect in a close circuit are now connected through a network, increasing their utility [6]. IoT sensor systems now allow the connection of physical objects so that remote services can be provided through the Internet by analyzing the data from these sensors. Thus, once the hardware of the IoT sensors is installed, programmers can provide new functionalities by developing new software based on different analyses.

In this paper we present a novel sensors system based on the IoT aimed at detecting memory losses for the early detection of some neurodegenerative diseases, by continuously assessing the memory of the user and notifying them when appropriate. Among other features of the system, we can highlight that this measurement method does not require any additional effort from the user, and is continuous. Users only need to go about their daily routine. The sensors system was installed in a cupboard, converting it into an IoT smart cupboard (SC). We used a normal cupboard, such as one that most readers could find at their home or in their kitchen. The SC had some door sensors connected to a Raspberry Pi, programmed to analyze the signals and measure the memory.

The main contribution of the current work over the related works of other authors is its presentation of a low-cost solution that can monitor users in their daily lives for measuring memory with the potential of detecting diseases with memory impairments, without needing qualified staff. In addition, the mechanism is novel, as this is the first work that presents a novel SC for this purpose, and is based on magnetic door sensors with very low prices. This work extends our previous work about IoT collaboration exemplified with a SC prototype [7]. The contribution of the current work over the previous one lies in the use of a more advanced three-door SC prototype that measures memory. This was proved with experimental results obtained from 23 participants in which the SC measurements correlated with a validated memory test and another test about self-perceived memory.

The current work is organized as follows. The next section reviews the existing related works considering the common technologies in this field. Section 3 describes the design of the proposed SC to assess memory and all its features. Section 4 describes the conducted experiments and the user tests for validating the system. Section 5 presents the main results. Finally, Section 6 discusses the results, draws conclusions, and depicts some future lines of research.

2. Related Work

The research community is actively involved in the topic of this work due to the consequences of memory losses on the wellbeing of patients and their social environments. The goal is to reduce their economic impact on the society due to treatment costs. IoT technology allows the interconnection of small low-cost devices practically anywhere. These devices can monitor health indicators and the

behaviors of people. There are many works and projects on this topic, and this section introduces the most relevant ones.

Some projects present solutions involving Alzheimer's disease and Raspberry Pi. For instance, Nonavinakere et al. [8] developed a system that recognizes a person's face and tells the user the name of that person and the relationship they have with them. The tool was developed thinking about users with Alzheimer's disease. The system was tested using three different platforms; one of them was a Raspberry Pi 3, and although it was not the fastest platform, it was the most accurate, since it was able to detect a person within certain limits. Crema et al. [9] proposed an embedded platform-based system for early detection of Alzheimer's disease through transcranial magnetic stimulation (TMS). TMS is a non-invasive way to stimulate the cerebral cortex in order to address Alzheimer's disease. This system was formed by a magnetic stimulus generator, an electric stimulus generator, a field-programmable gate array, and a Raspberry Pi. The goal was to introduce an alternative technique that supported the early detection of Alzheimer's with reduced costs, and provided results that were suitable for medical interpretation. Narendiran et al. [10] developed a cognitive assistance system for smart homes. The main aims of the project were (a) to simulate the progression of Alzheimer's-type dementia by evaluating performance in the execution of an activity of daily living and (b) to provide support for impaired people who need help in daily activities such as preparing a cup of coffee. The system used a camera connected to Raspberry Pi. The camera provided live images to the Raspberry, whose contents were the patient inside the home environment. While the Raspberry was receiving images, it assessed the performance of a task and provided feedback to the patient about their performance. For instance, when a patient forgot some step of some task, the system reminded the patient about this step. Ishii et al. [11] designed an early-detection system for dementia using the Machine-to-Machine (M2M)/IoT platform. The system was formed by sound sensors, motion sensors, pressure sensors, an Arduino board per sensor, a Raspberry Pi board, an M2M server, and the corresponding analysis software. The authors assessed several activities and behaviors of a person inside their home. Several sensors were set up in the home environment, including outdoors near the home and inside some rooms (e.g., bedrooms, bathrooms). Each Arduino board connected to a sensor sent information to the Raspberry Pi. This had two functions; the first was to send information to the M2M server, and the second was to analyze the collected information through the analysis software in order to determine early symptoms of Alzheimer's disease. It is worth highlighting the mixed use of Arduino and Raspberry Pi boards. Kristalina et al. [12] kept in mind one of consequences of memory impairment, which is that a certain person can forget where they are. In order to address this handicap, they developed a system that involved a Raspberry Pi and an iBeacon. This was a tracking system for patients with memory impairment. Each patient carried an iBeacon device that was responsible for sending the ID and signal strength to the Raspberry Pi and then to the server in order to convert the information to a distance. Due to the amount of noise, it was possible that the obtained distance data did not match with current patient position, so the authors applied the Kalman method in order to estimate the distance between devices. This system was assessed at the Dr. M. Soewandhie hospital, and their tests showed an average percentage measurement error of 7.01% in the actual patient position. Chavan and Chavan [13] proposed a novel system for fall detection in elderly people. They benefited from the new features of Raspberry Pi 3 with respect to the previous version (i.e., Wi-Fi connection) for the creation of a new system with wearables. The system was formed by a laptop, a Raspberry Pi 3, accelerometers, a heart rate sensor, and a temperature sensor. The sensors sent information to the Raspberry, and this determined if there had been a fall. If so, a text message was sent to a mobile device. Paul et al. [14] described a low-cost system for monitoring patients, which was formed by several sensors, a Raspberry Pi, a database, and an application. The system's aim was to collect patient data (e.g., electrocardiogram signal, blood pressure signal, heart rate signal, blood oxygenation, temperature) in order to send them to the patient's doctor. The system was set up in Bangladesh with success.

Although they do not make use of a Raspberry Pi, the following projects addressed Alzheimer's disease with other IoT elements. Chong et al. [15] proposed a system in order to predict a potential Alzheimer's medical condition. They used a room with movement sensors inside it and analyzed the data obtained from 20 elderly persons by means of five sensors over the course of six months. The results provided three key factors in order to perform a prediction: excess activity levels, sleeping patterns, and repetitive actions. These factors were useful for predicting the early warning signs of Alzheimer's, and allowed the authors to provide recommendations to caregivers based on the prediction analyses. Navarro et al. [16] developed a fuzzy adaptive cognitive stimulation therapy generation system for Alzheimer's patients. The aim of the system was to reduce the cognitive burden of care workers and therapists. The system assessed patient behavior through several activities and even through their voice tone and their phrases. This system used the Mente Activa software, whose aim was to provide computer-assisted cognitive therapy. The authors demonstrated the enhancement of patients with the experiments with their system. Finally, Roopaei and Jane [2] focused on another aspect related to memory loss, which was the ability to recognize familiar faces. The authors developed a platform to support patients who suffered from face perception impairment with an assistive intelligence device. The system included an algorithm that recognized a face among entries in a face dataset. The algorithm used deep learning to recognize patterns in faces and match them. Regarding IoT, the authors proposed to use glasses in order to let the user know who was in front of them as well as their relationship.

Table 1 depicts the main differences and similarities of the current work with the most related ones. As one can observe, the current work is the only one that has all the following four features at the same time: (a) it does not need qualified staff, and hence anybody can use it without previous experience; (b) it has the potential to measure memory by just analyzing the daily activities of users; (c) it is a low-cost solution for monitoring; and (d) it can detect symptoms of memory disease in early stages. The most similar work is the one by Ishii et al. [11], as it also has the potential to measure memory and conduct the early detection of memory-impairment related diseases by analyzing daily activities without requiring qualified staff. Even though, the current work has all these features, it is also low cost, thanks to the novel mechanism based on a SC with very low-cost magnetic door sensors.

Considering all the related works presented in this section, we also noticed a gap in the literature about using pieces of IoT-enabled furniture for monitoring the memory of users for the early detection of memory-impairment diseases. The current approach covers this gap in the literature by presenting an IoT SC, built with low-cost magnetic door sensors, introduced in the next section.

Table 1. Comparison between the current work and the most closely related ones.

Question	Current Approach	Nonavinakere et al. [8]	Crema et al. [9]	Narendiran et al. [10]	Ishii et al. [11]	Paul et al. [14]
Does this work use IoT?	✓	-	-	-	✓	
Does this work use Raspberry Pi?	✓	✓	✓	✓	✓	✓
Does this work present a low-cost solution for health monitoring?	✓	✓	-	-	-	✓
Does this system use wearable devices?	-	✓	✓	-	-	✓
Can this solution be applied without qualified staff?	✓	-	-	-	✓	
Does this solution measure memory?	✓	-	-	-	✓	
Does this solution measure cardiac measures? (heart rate, heart rate variability)	-	-	-	-	-	✓
Does this solution measure temperature?	-	-	-	-	-	✓
Does this solution have the potential to measure any health indicator by just analyzing the daily activities of users?	✓	-	-	✓	✓	✓
Does this solution have the potential to measure memory by just analyzing the daily activities of users?	✓	-	-	✓	✓	
Could this solution help to detect memory-impairment diseases at an early stage?	✓	-	✓	✓	✓	

3. Smart Cupboard for Assessing Memory

In Figure 1, the reader can observe a picture that depicts the overall experiment described in this paper. This paper also presents the design of the SC, the assessment method of the SC, and the experimentation with users. The core of the system is formed by a Raspberry Pi model 3 B+, with CPU 1.4 GHz 64-bit quad-core ARMv8, 1 GB Memory (SDRAM) (shared with GPU), 17x GPIO and HAT ID bus, 5 V through MicroUSB or a GPIO header. A lithium-ion battery accompanies the Raspberry Pi, which facilitated the setting up of the system inside the cupboard for the experiments, since a wire connected to power was not necessary. This provided the possibility of installing the sensors system in a cupboard without needing a nearby socket. The autonomy of the battery was 9 h, and we considered that this was enough to assess our system in controlled environments with users. The SC also had magnetic door sensors. The cupboard selection was made based on certain features. The requirements that the furniture must have according to our controlled experiments were (a) to be placed in a kitchen, (b) to have three compartments of the same size (to avoid memory techniques based on the size of objects and compartments), and (c) that each compartment could hold 5 to 10 items without overlapping (to facilitate the acquisition phase based on observation). We used an Excellway MC-38 wired magnetic alarm system door window sensor switch with screw provided by Banggood. Figure 2 shows this magnetic door sensor. Each sensor was composed of two parts; one was attached to the cupboard structure and connected to the Raspberry Pi, and the other was attached to the door, such that both parts were together when the door was closed and apart when it was open. Each sensor closed the circuit when both parts were together (or very near to each other). For our system, we used three pairs of sensors and these were set up in the three doors of the cupboard. A protoboard and

jumper wires were used to connect the Raspberry Pi and door sensors, and the schematic design is presented in Section 3.1. We wrote a Python script in order to manage the proposed SC. The script assessed the memory of users based on the analysis of the signals of door sensors, with the algorithm described in Section 3.2.

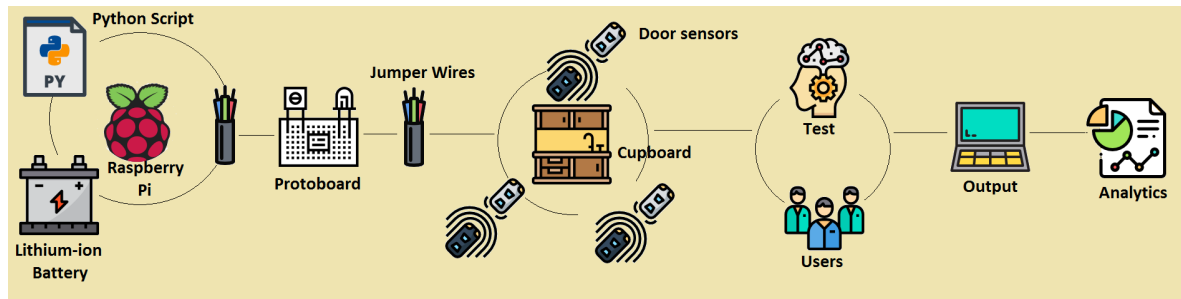


Figure 1. Overview of the smart cupboard and the experiments.



Figure 2. Door sensor.

3.1. Schematic Design of the Smart Cupboard

The door sensors and the Raspberry Pi were connected through jumper wires and a protoboard, and this section explains in detail how these elements were connected. The Raspberry Pi had a pin series placed on a side of the board, called GPIOs (general-purpose inputs/outputs). They performed multiple input/output operations for different purposes. The Raspberry Pi model used in this work had 40 pins. Figure 3 depicts the schematic design of the SC, indicating the used pins. This schematic design uses the following color notation to distinguish the different pin types:

- Red pins: power to 3.3 V and 5 V.
- Green pins: Communication through Inter-Integrated Circuit (I2C) protocol in order to communicate with peripherals that use this protocol.
- Blue pins: Connection for the universal asynchronous receiver–transmitter (UART) for a conventional serial port.
- Black pins: Connection to ground.
- Orange pins: Communication through the Serial Peripheral Interface (SPI) protocol in order to communicate with peripherals with this protocol.
- White pins: Reserved pins.
- All GPIO pins: Apart from their particular function, all GPIO pins have general-purpose inputs/outputs.

Each door sensor had two wires and, due to their specification, one of these wires needed to be connected to ground and the other one needed to be connected to some input. Pins GPIO 18, GPIO 12, and GPIO 25 were chosen as input pins; pins GPIO 14, GPIO 20, and GPIO 30 were selected as ground pins. These choices were mainly arbitrary, and we only considered that chosen pins with inputs/outputs had a ground pin next to them. Because wires of door sensors could not be

directly connected to the Raspberry Pi, we connected these through a protoboard by means of jumper wires. As one can observe in the schematic design, all ground pins were connected through jumper wires to the positive power line of the protoboard (representing this connections with black lines). Then, in order to ensure the connection continuity until the door sensors, a jumper wire was placed from the power line to the central segment of the protoboard for each sensor. In the schematic design, these connections are represented with black lines that go from the “+” column to the “A” column. Finally, door sensors were connected to the circuit through column “E”. It was necessary to use one or several jumper wires in this last step, depending on the distance from the protoboard to each door sensor. Input GPIO pins were directly connected to the protoboard through the central segment, then door sensors were connected with them through the same central segment (represented with yellow lines).

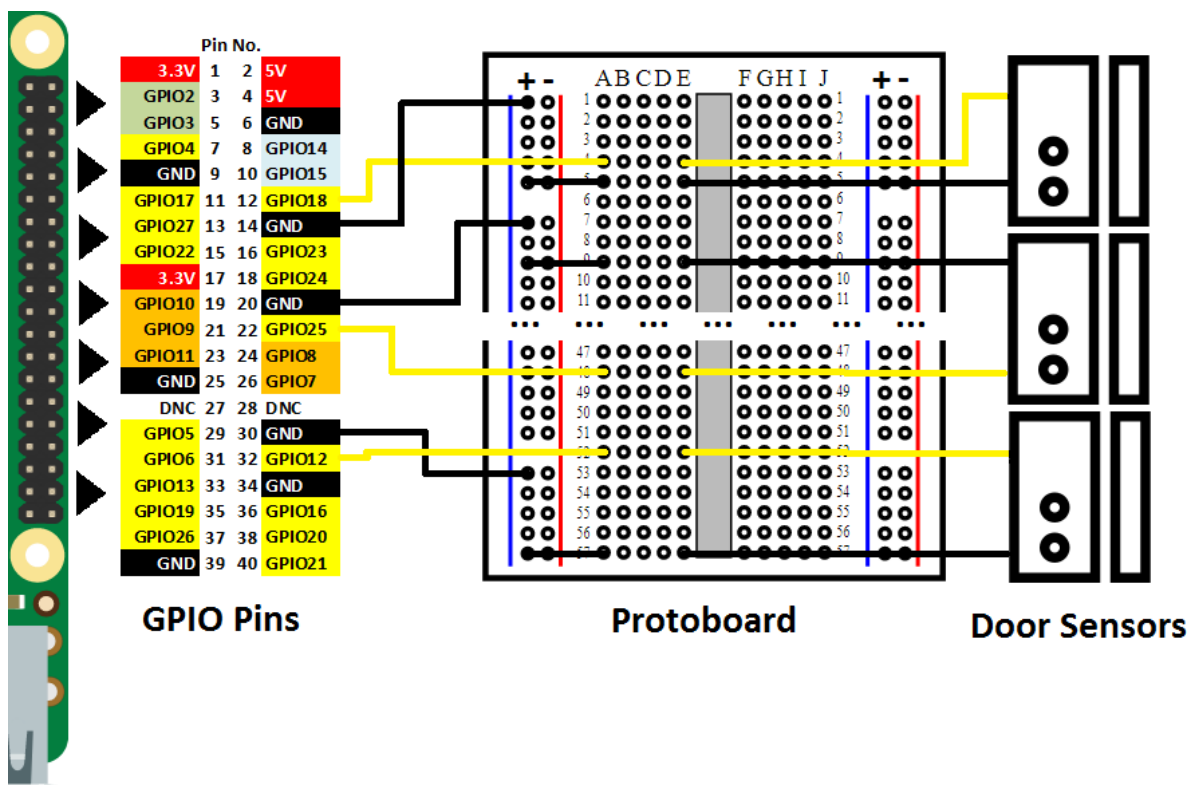


Figure 3. Schematic design of the smart cupboard. GPIO: general-purpose input/output.

3.2. Algorithm for Measuring Memory Based on the Door Sensor Signals

The algorithm was designed to determine when a user finds an item, and when the user searches for an item without success. One research question was: how do we know that the user had success in searching an item inside the SC? In order to answer this question, we had to explain all possible cases in which a user can find an object. The first case is that the user finds a certain item in the first attempt. The second case is that the user finds a certain item in a certain number (denoted as N) of attempts, assuming $N \geq 2$. The last case is the one in which the user did not find the item.

Figure 4 depicts the first case. One of the rules that allows understanding this topic is that the user usually has success in finding objects except in some cases. Nonetheless, we do not know how many times the user has attempted to find a certain object. In this first case, the user is going to find a certain object at the first attempt. With the open door of the SC, the user looks and searches for the desired object. Once the user grabs the object, they close the door and at this moment, our script takes note of one fail with the search. It seems illogical that our system would increase the fail counter, but since we do not have another mechanism to determine exactly whether the user has grabbed the desired item or to know whether the user has found the desired item (assuming this reduced set of

low-cost sensors), our system marks one fail. However, we kept in mind that if the user does not open another door or the same door in a reasonable amount of time, the most probable reason is that the user found the item. We established 10 s as reasonable amount of time, and hence once the door of the SC was closed and 10 s passed, we estimated with high probability that the user had the desired item. When the door is closed, besides increasing the fail counter, the “closeDoor” signal is triggered, which starts a time counter that allows us to know whether the user opens a SC door in a reasonable time or not. Since we are explaining the case in which an object is found at the first attempt, this time the counter is not interrupted. In following cases we will explain what happens when this signal is interrupted. So, when the system notices that after 10 s the user has not opened any door, it removes a fail from the fail counter and increases a unit on the success counter.

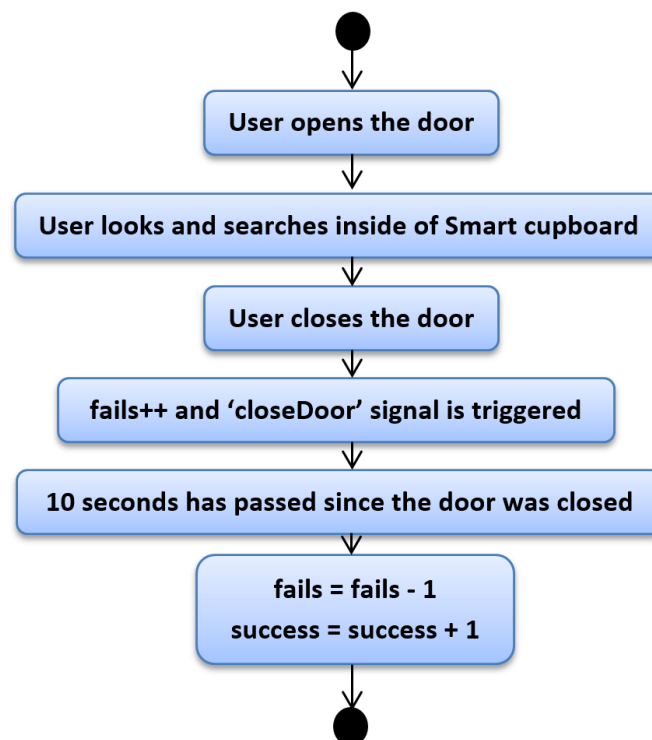


Figure 4. Python script—First case.

The second case is more complex than the first one. We will explain the same steps as above, but with more signals and certain features. In the second case, the user finds a certain item after N attempts. The beginning is the same as the previous case, as one can see in Figure 5, which depicts the diagram of the second case. The user opens the door, and before they search or find anything, the “openDoor” signal is triggered. The aim of this signal is to determine whether another door has been opened before, and in the positive case our system cancels the count of 10 s in order to avoid reducing the fail counter and to prevent increasing the success counter. In this way, our system counts all fails during the process of searching for an item. Focusing again on this second case, we take for granted that the “openDoor” signal has not been triggered, since it is the first time that the user opened the door. Nonetheless, the action of opening the door is the trigger of the “openDoor” signal. The same signals as in the previous case are also triggered, but we have omitted them in this description in order to ease comprehension.

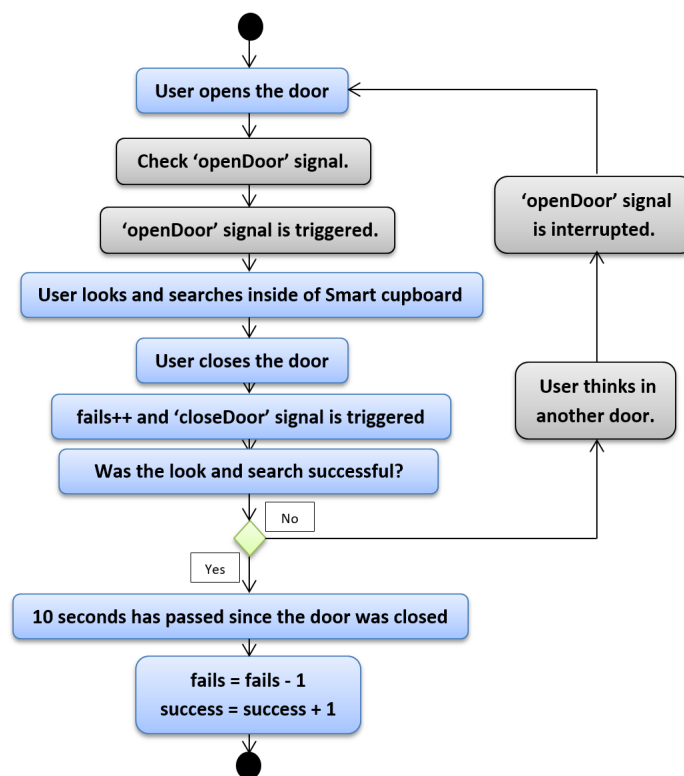


Figure 5. Python script—Second case.

When the “openDoor” signal is launched, the user starts searching for the item, then they close the door. The fail counter increases and the “closeDoor” signal is triggered, and until this point, all steps are the same as in the first case. Now, the user knows whether they have the correct item. If so, it is the first case; if not, the “openDoor” signal must be interrupted. Empirical tests made by ourselves and other users allowed us estimate that 10 s was enough time for someone to be able to open another door of the SC; if not, again, it was assumed that the user found the correct item. Hence, in the second case when the user thinks about what their next door choice will be and opens it, the “openDoor” signal is interrupted and the cycle starts again until the user opens the correct door. Until this moment the user has always had success in searching for their object, regardless of whether it was found in their first attempt or in attempt N . However, in the following case the user does not have any success, since according to our point of view the user does not reach to find the required object. We kept the third case in mind in order to manage two issues: the first is that the user searches for an object but forgets what they were searching for. This situation gives us information about the health of the user’s memory. The second is that in this way we can avoid that someone cheated during the experimentation phase (i.e., if we did not control the opening time of a door and a certain object was not inside the SC, the user would have unlimited time to think about what other compartment the object may be in). In the experimentation phase, this case did not appear at any moment, but it is important to check for this issue because it makes the measurement of memory loss more accurate.

Figure 6 depicts the third case. The beginning is the same as aforementioned cases, only with the difference that another signal is triggered when the door is opened by the user; this signal is called “countTimeDoor” (we have not mentioned the signal before in order to avoid over-long explanation, but it was also present in the previous cases). The signal’s aim is to start to count the time that an SC door is held open. This period of time matches with period of time the user is searching an object inside of the SC. The assigned threshold for this signal was 10 s, that is, the user has 10 s to find the item, and if this time is surpassed the system increases the fail counter. We determined the threshold of the “countTimeDoor” signal in the same way as we determined the 10 s in order to know whether user was successful (i.e., through experiments made by ourselves and other users), until we were able

to determine a proper threshold. We assume that the user overcame the signal threshold, so the fail counter increases. Furthermore, the “openDoor” signal is canceled, since if it were not so, when the user closed the door again, our system would increase the fail counter once again. Finally, it is worth mentioning that if the user closes the door before 10 s, the “countTimeDoor” signal is canceled in order to avoid increasing the fail counter twice.

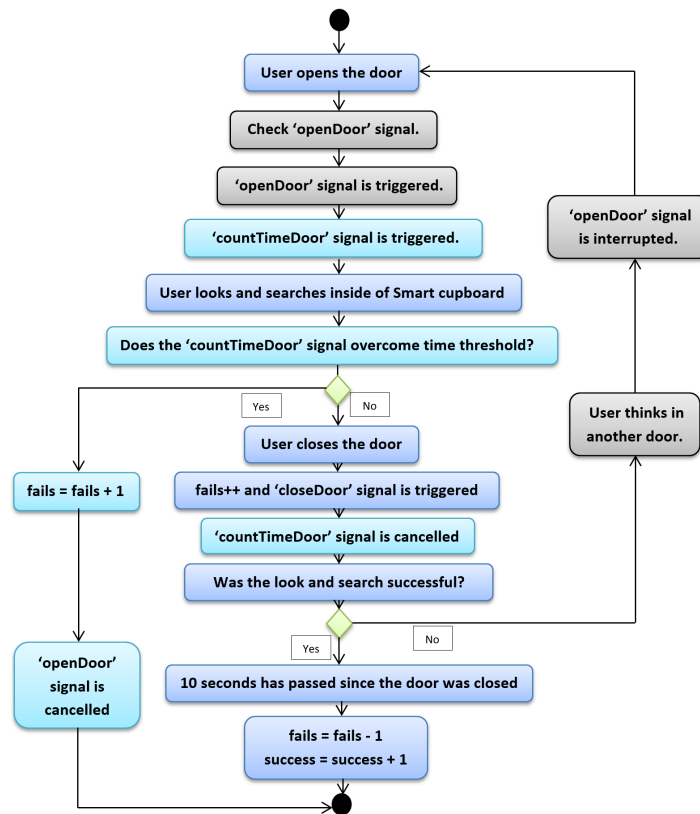


Figure 6. Python script—Third case.

The algorithm was written in Python, and for the sake of reproducibility, we describe how the implementation of this algorithm handled the pins. In order to manage pins inside the script, we used the RPi.GPIO library. There were two options to enumerate the pins. The first was GPIO mode, in which each pin had the same number as their physical position, hence pins were enumerated from 1 to 40. The second option was BCM (Broadcom mode), in which pins were numerated in order to match with Broadcom chip, which was the CPU (central processing unit) of the Raspberry. We used BCM for the implementation of the presented algorithm. The algorithm implementation also needed to set up some pins as input pins, and this was achieved with the predefined function GPIO.setup. Finally, the GPIO.input function provided the current state of each door sensor, true when the two pieces of a door sensor were separated (i.e., the door was open), and false otherwise. Figure 7 presents an excerpt of the Python implementation used in the SC, showing the aforementioned implementation details about pins. Door sensor states were used as previously described when presenting the algorithm.

```
01. import RPi.GPIO as GPIO
02.
03. #Set broadcom mode so we can address GPIO pins by number
04. GPIO.setmode(GPIO.BCM)
05.
06. #This is the GPIO pin number we have one of the door sensor
07. #wires attached to, the other should be attached to a ground
08. DOOR_SENSOR_PIN_ONE = 18
09. DOOR_SENSOR_PIN_TWO = 12
10. DOOR_SENSOR_PIN_THREE = 25
11.
12. #Set up the door sensor pin
13. GPIO.setup(DOOR_SENSOR_PIN_ONE, GPIO.IN, pull_up_down = GPIO.PUD_UP)
14. GPIO.setup(DOOR_SENSOR_PIN_TWO, GPIO.IN, pull_up_down = GPIO.PUD_UP)
15. GPIO.setup(DOOR_SENSOR_PIN_THREE, GPIO.IN, pull_up_down = GPIO.PUD_UP)
16.
17. while True:
18.     oldIsOpenOne = isOpenOne
19.     isOpenOne = GPIO.input(DOOR_SENSOR_PIN_ONE)
20.
21.     oldIsOpenTwo = isOpenTwo
22.     isOpenTwo = GPIO.input(DOOR_SENSOR_PIN_TWO)
23.
24.     oldIsOpenThree = isOpenThree
25.     isOpenThree = GPIO.input(DOOR_SENSOR_PIN_THREE)
```

Figure 7. Implementation details about pins in the Python script of the smart cupboard.

4. Experimentation

4.1. Participants

We recruited 23 people for participation in this user study. Participants were 36.17 years old on average (SD = 12.80) in a range from 18 to 60 years old, and had studied for 14.86 years on average (SD = 2.88). Among the participants, only 8.69% were studying or work in computer science. Males comprised 39.13% of participants. Participation in this experiment was voluntary and unpaid.

4.2. Procedure

In order to evaluate whether the SC is able to measure memory, several tests were conducted. In the first test, a user was asked to observe the inside of the SC. The user had to memorize certain items inside it in the acquisition phase. Then, the user was asked to find certain items in the retrieval phase. A test of face–name pairs [17] was used as a control method, since this kind of test has been proven to measure memory. The test consists of showing a list of face–name pairs, so the user memorized them in the acquisition phase, for later selection of the name associated with each face in the retrieval phase. The main goal was to determine whether both results were correlated, besides performing other analyses concerning the relation of the results with the participant features.

The test was conducted in a real kitchen so that participants were familiar with the scenario. The Raspberry was set up inside a kitchen cupboard as shown in Figure 8. The size of this cupboard was 130 cm width × 71 cm height × 29.5 cm depth, and it was 150 cm above the ground. In spite of having five compartments, we only used the bottom three in order to avoid having compartments of different sizes.



Figure 8. Smart cupboard.

To assess the memory of participants with the SC, we selected 30 different items. All these items were typical objects commonly found inside cupboards, and these objects were: a cup, a sweet corn can, a chili can, an egg, a box of matches, an evaporated milk carton, a soda, a bag of breadcrumbs, a beer can, a jar of chili peppers, a potato, a jar of lentils, a can of olives, a jar of mayonnaise, a carton of chocolate milkshake, a can of grapes, a jar of soup cubes, a can of peaches in syrup, a can of condensed milk, salt, a box of baking powder, a can of green peas, a milk bread, a jar of jam, a teaspoon, a jar of sausages, honey, a can of tuna, a bag of tea, and a jar of oregano. In this experiment, each participant followed the same process. The experimenter introduced the steps briefly to each user. In the acquisition phase, the experimenter asked each user to memorize all the items of each compartment, and they had 30 s per compartment—1 min and 30 s in total.

In the retrieval phase, the experimenter told the participant that he would ask them to find objects selected in a random order from the ones inside the cupboard and previously memorized by them. Thus, the participant had to open the compartment where they thought each required object was. Furthermore, the experimenter indicated that only one door could be open at a time (i.e., before the participant opened another door, they had to close the current door). Once the participant had found the required object, grabbed it from the SC, and closed the door, the experimenter asked questions about the item. The questions were varied and related to cooking or eating. For instance, what recipes or dishes would you cook with this object? Or, what time of day do you usually eat this product? Or, do you think this product is healthy and why or why not? And so on. The reasons for these questions were to delay the retrieval phase and to increase the difficulty of the test. When users opened the door in order to find an object, they could re-memorize where each object was (reinforcing the initial learning), since it was unavoidable to let them see the contents again. Thus, the goals of these distracting questions were to compensate for this aspect and to be more similar to realistic daily conditions.

This process was repeated with ten different objects for each user. Due to the size of SC and the amount of items, two rounds were required. In each round, each participant had an acquisition phase in order to memorize the content of compartments concerning 15 objects, and had a retrieval phase to sequentially find 10 objects. When the first round was finished, the experimenter asked the user to leave the kitchen. While the participant was outside the kitchen, the experimenter set up the second round, and then invited the participant to come into the kitchen again. Hence, users performed 20 memory retrievals about 20 different objects. In this way, this memory test had an accuracy error margin of 5%, which is considered as appropriate in memory tests [18]. We decided that all participants had the same conditions; hence, before starting this procedure, a list of items was selected for use by all participants.

The list had 15 items for the first round and 15 items for the second one. The order of objects was selected randomly, because we wanted to avoid the case where objects were organized by size or semantic categories, in order to avoid bias in the memory measurement due to different memorization techniques. Table 2 indicates the order of objects in the SC, distributed in compartments per round. Furthermore, another requirement of the experimentation phase was that objects could not be behind others (i.e., all objects had to be visible from the participant's position). The experimenter was always with the participants, except when they were outside the kitchen. The experimenter made sure that the participants properly followed the experimentation protocol. For instance, the experimenter was advised to take note if any participant closed the door twice because it had not been closed with enough strength the first time. In this case, the system would register an additional fail, so then we could revise the logs to know what had happened.

Table 2. Order of objects in the experimentation with the smart cupboard.

Object	Compartment	Round	Object	Compartment	Round
Cup Sweet Corn Chili Egg Box of Matches	First	First	Grapes Soup cubes Peaches in syrup Condensed milk Salt	First	Second
Evaporated milk Soda Breadcrumb Beer Chili peppers	Second		Baking powder Green peas Milk bread Jam Teaspoon	Second	
Potato Lentils Olives Mayonnaise Chocolate milkshake	Third		Sausages Honey Tuna Tea Oregano	Third	

The next step for participants was to take a control test based on face–name pairs in order to statistically compare these results with the SC results and to determine whether our SC is able to measure memory. This test was similar to the common memory tests about face–name pairs in the literature [17,19], and we used a short-time version that did not require several days for acquisition and retrieval phases. In this way, each participant could do all the experimentation in the same day, facilitating the task of recruiting unpaid volunteer participants. In this experiment, the test of face–name pairs consisted of showing a series of 30 face–name pairs to the participant such that they memorized these associations in the acquisition phase. Each face–name pair was presented to the user for 6 s, and consequently the whole acquisition phase took 3 min. In the retrieval phase, each participant had to respond to 30 questions. Each question was composed of a face image and four name options, and the participant had to fill a form provided by the experimenter with the answers to these questions. Figure 9 shows an example of three questions. The face images have been blurred in this article to protect the privacy of the models. The retrieval phase had no time limit, but the experimenter instructed the participants to reply to the questions as accurately and quickly as possible, and the reaction time was measured.

Furthermore, the participants engaged in a self-reported memory test. We performed this test in order to compare the SC results with other memory-related variables. Since the self-assessment of memory has proved to be relevant for evaluating memory despite other influencing factors such as personality [20], we included this brief self-reported memory test as another control test. We selected a short self-reported test available from the Psychology Today website (<http://psychologytoday.tests.psychtests.com/bin/transfer?req=MTF8MzM2MHw2NzI5MDI0fDB8MQ==>) for its brevity and its simplicity. In this test, participants replied to seven questions with a five-point Likert scale. The questions of this test were: (1) Do you have difficulty in remembering people's names or phone

numbers? (2) How often do you find yourself trying to remember the location of everyday items (e.g., your keys, wallet, glasses, etc.)? (3) How often do you have to replace passwords (numerical or verbal) because you've forgotten the original one? (4) How often do you find yourself asking questions like, "What was I about to do next?" (5) How often do you end up arranging overlapped plans because you forgot you had made previous plans with someone else? (6) How often do you have to ask someone to repeat instructions or a story because you can't remember what was said the first time? (7) How often do you have difficulty in remembering where you parked your car? The last question was only replied by participants who had a driving license.

The experimenter also asked participants to reply a brief demographic test to extract the information presented in Section 4.1 when introducing the sample of participants. Once we finished all the experimentation with all the participants, we analyzed the obtained data as described in the next section.

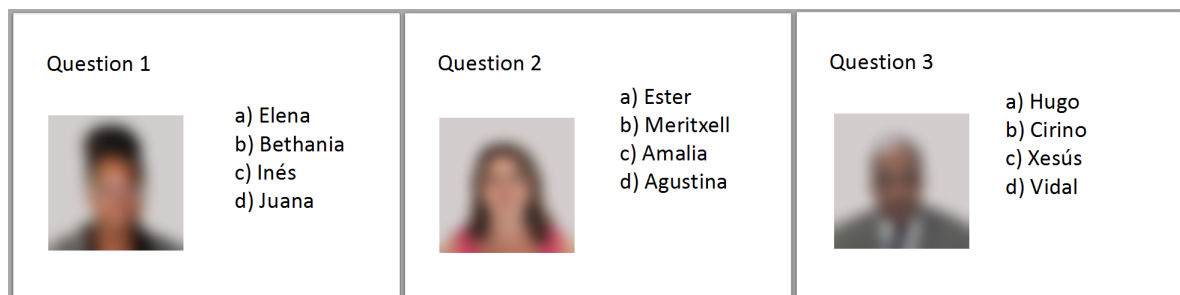


Figure 9. Test of face-name pairs.

5. Results

We performed several analyses considering the memory measurements in the different methods, the reaction time, and the age of participants. Firstly, we compared the memory measurement results between the SC test and the face-name test, reporting the accuracies of participants in the retrieval phase.

In order to double-check that the sensors system of the SC was working properly, the experimenter took notes about the fails and successes of participants during the experimentation phase, and then the notes were contrasted against the system log. The notes and SC logs and results matched perfectly. The accuracy percentage of each participant was calculated as shown in Equation (1) as a measurement of their memory:

$$a = \frac{s}{s + f} \cdot 100, \quad (1)$$

where a is the accuracy percentage, s is the number of successes, and f is the number of fails.

The accuracy of each participant in the retrieval of face-name pairs was calculated in a similar way. The experimenter checked the final test results, and the percentage was calculated as shown in Equation (2):

$$a = \frac{s}{n} \cdot 100, \quad (2)$$

where a is the accuracy percentage, s is the number of successes, and n is the total number of questions.

Figure 10 compares the memory accuracies of the SC and face-name pairs, and one can observe that both measurements methods followed similar trends and shapes. Thus, there may be a correlation between these measurement methods. In order to statistically and reliably corroborate this correlation, we conducted a Pearson's correlation test between the results of the two memory measurement methods. Table 3 shows the results of this correlation test. According to the Pearson correlation coefficient [21], both memory measurement methods had a significant positive correlation. This positive correlation was confirmed with the Kendall's tau coefficient of 0.470 with a p -value of 0.003 and Spearman's rho coefficient of 0.620 with a p -value of 0.002. The correlation between the SC test and the

test of face–name pairs proves that our SC sensors system is able to measure memory, since the control memory measurement method has already been scientifically validated.

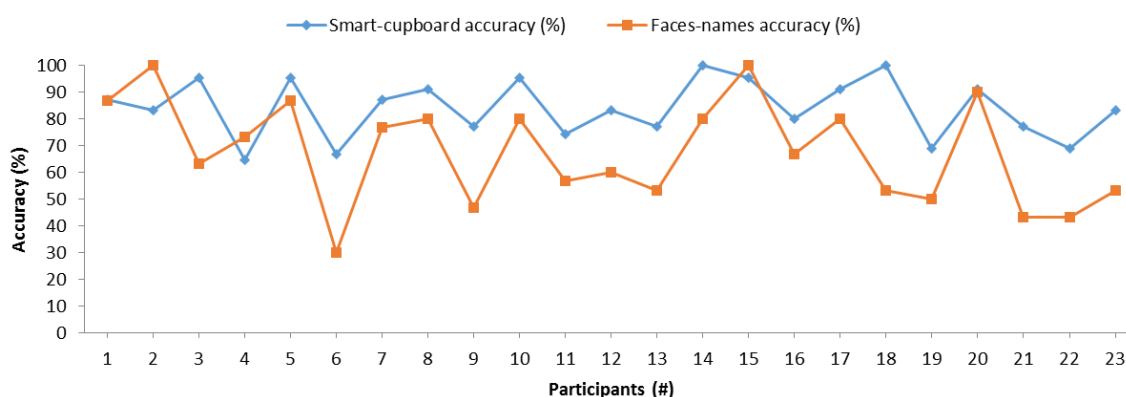


Figure 10. Comparison of memory measurements between the smart cupboard (SC) and the face–name pairs test.

Table 3. Correlation between the accuracy of the SC and the accuracy of the face–name test.

		Accuracy Smart Cupboard	Faces-Name Test
Accuracy Smart Cupboard	Pearson Correlation	1	0.597 **
	Sig. (2-tailed)		0.003
	N	23	23
Faces-Name Test	Pearson Correlation	0.597 **	1
	Sig. (2-tailed)	0.003	
	N	23	23

** . Correlation is significant at the 0.01 level (2-tailed).

Moreover, we analyzed the reaction time of participants in the SC and face–name pairs tests. Figure 11 depicts the reaction time of each participant in both tests. The blue line represents the SC test and the orange line represents the test of face–name pairs. In order to calculate the reaction time of the SC test, the experimenter took note of the time spent by a participant to remember each item inside the SC. Then, this was compared with the time in the system log in order to check that all times were correct. Thus, 20 reaction time results were obtained for each participant. Finally, the reaction time of each participant was calculated as the mean of all obtained times. In the face–name test, the experimenter also measured the time spent by a participant in order to perform the test. The reaction time was obtained from the division of the total time by the total number of questions by each participant. According to the trend and direction of both lines in the graph, it is not easy to appreciate the similarity in general. Nonetheless, a certain similar behavior is appreciated between participant 7 and participant 15. A similar correlation can be appreciated between these two tests, since both lines are almost parallel. Because this observational analysis is not sufficient to determine whether there was any significant relation between tests in reaction times, we performed another Pearson’s correlation test to statistically determine whether there was a statistically significant correlation. Table 4 depicts the result of the correlation test. It shows that both variables were not significantly correlated. Neither Kendall’s tau coefficient nor Spearman’s rho coefficient detected any significant correlation with respective p -values of 0.597 and 0.428. Thus, in these experiments, the reaction time of our SC test did not correlate with the reaction time of the control test of face–name pairs.

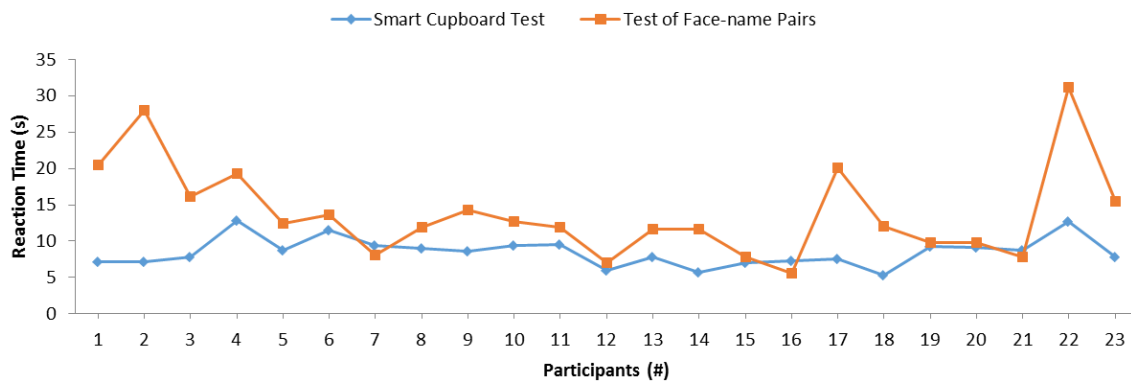


Figure 11. Comparison between the SC reaction time and the reaction time of the face–name test.

Table 4. Correlation between the SC reaction time and the reaction time of the face–name test.

		Reaction Time Smart Cupboard	Reaction Time Face-Name Test
Reaction Time Smart Cupboard	Pearson Correlation	1	0.341
	Sig. (2-tailed)		0.111
	N	23	23
Reaction Time Face-Name Test	Pearson Correlation	0.341	1
	Sig. (2-tailed)	0.111	
	N	23	23

We also conducted an analysis of the relation between participant age and SC reaction times. Figure 12 represents each participant considering these two aspects. It is worth highlighting that we asked people to participate in these experiments, considering their age, to have both young and aged people. In particular, there were six young participants in the 18–25 years old range and six aged participants in the 55–60 years old range. In order to determine whether there was a statistically significant correlation, we performed three correlation tests between SC results and age. Table 5 shows the results of the Pearson’s correlation test. One can observe that these variables were not correlated according to this test. In addition, neither Kendall’s tau coefficient nor Spearman’s rho coefficient detected any significant correlation, with respective *p*-values of 0.265 and 0.300. Thus, SC results and age were not statistically significantly correlated in these experiments.

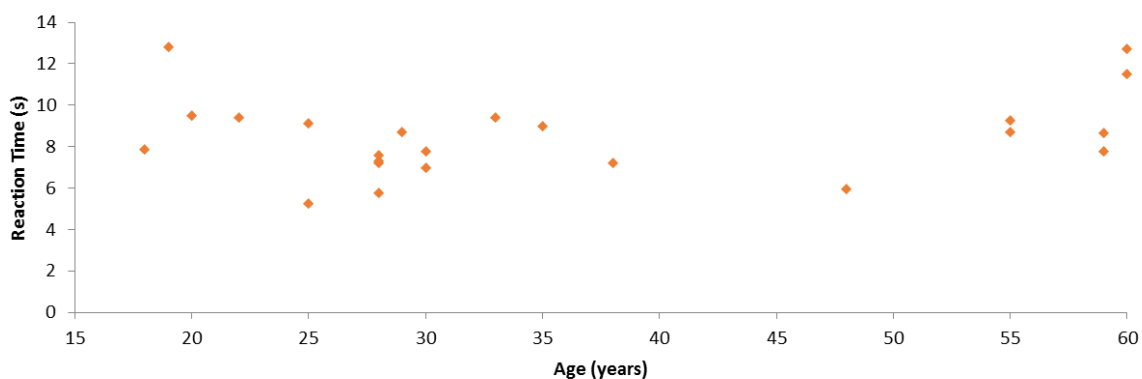


Figure 12. Comparison between the reaction time in the smart cupboard test and participant age.

Table 5. Correlation between the reaction time and participant age in the smart cupboard test.

		Age	Reaction Time Smart Cupboard
Age	Pearson Correlation	1	0.306
	Sig. (2-tailed)		0.156
	N	23	23
Reaction Time Smart Cupboard	Pearson Correlation	0.306	1
	Sig. (2-tailed)	0.156	
	N	23	23

We also performed an analysis comparing the accuracy of participants in the SC test and the results of the self-reported memory test. Each possible answer of the self-reported memory test among the options “almost always”, “often”, “sometimes”, “rarely”, and “almost never” were respectively assigned the values 0, 1, 2, 3, and 4. The results of this test were standardized as a percentage calculated with Equation (3):

$$r = \frac{\sum_{i=1}^n x_i}{n} \cdot \frac{100}{V_{max}}, \tag{3}$$

where r is the result of the self-reported test, x_i is the value of each answered question, n is the total number of questions, and V_{max} is the maximum value that a response can have (i.e., 4 in this case).

Figure 13 shows the accuracy of the SC test and this self-reported test. There were similarities between both tests in some cases, as one can observe in the intervals between participants 1 to 4, participants 9 to 11, and participants 15 to 17. To determine the statistical significance of this relation, we conducted a Pearson’s correlation test, and Table 6 presents the results. The test indicated that the memory results between the SC test and the self-reported one were significantly correlated. This correlation was confirmed with the Kendall’s tau coefficient of 0.383 with a p -value of 0.014 and Spearman’s rho coefficient of 0.451 with a p -value of 0.031. The self-reported test is a subjective test, and personality may cause bias in the results, since this test actually measures self-perceived memory rather than actual memory (calculated as the accuracy retrieving information previously acquired). According to these experiments, the SC results were correlated with self-perceived memory, despite the possible bias because of personality.

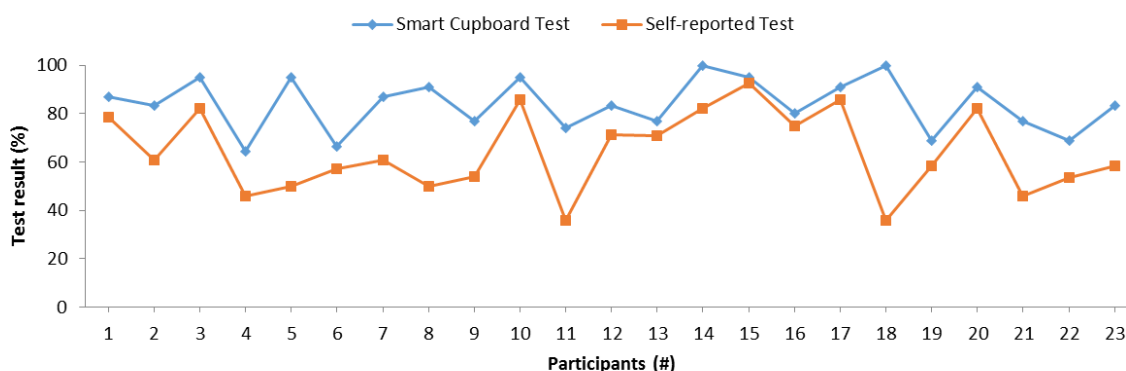


Figure 13. Comparison between the accuracy of SC and that of self-reported tests.

Table 6. Correlation between the accuracy of SC and that of self-reported tests.

		Smart Cupboard	Accuracy Self-Reported Test
Smart Cupboard	Pearson Correlation	1	0.443 *
	Sig. (2-tailed)		0.034
	N	23	23
Accuracy Self-Reported Test	Pearson Correlation	0.443 *	1
	Sig. (2-tailed)	0.034	
	N	23	23

*. Correlation is significant at the 0.05 level (2-tailed).

6. Discussion and Conclusions

The article proposed a new mechanism of measuring memory with the SC as a novel IoT sensors system. We presented the design of the SC as a cupboard with three sensorized doors with magnetic door sensors connected to Internet via a Raspberry Pi 3B board with the corresponding software for evaluating user memory.

The main goal was to have a device able to assess the memory in a familiar environment without requiring additional effort from the user. Thus, we presented a solution in which the memory measurement can be continuous and based on normal routine. The results based on 23 participants in a wide age range (18 to 60 years old) showed that the accuracy of participants in finding objects in the SC in a controlled environment was statistically significantly correlated with the accuracy of participants in retrieving face–name associations in a validated type of memory test. The accuracy of the SC test was also statistically significantly correlated with a self-reported memory test.

The current work attempted to find a solution that was low-cost as possible, in order to propose a step towards a solution that can get to the market with a profitable margin, so that enterprises may be interested and our solution can make a real impact on society. Note that the most fundamental components of this solution were the magnetic door sensors, and in particular we used a door sensor model that only cost \$2.46. The Raspberry Pi 3B board could be easily replaced by any other low-cost/green processing board in the market by using the same software and adapting the input pins. Thus, a very cheap solution could potentially be developed for converting a cupboard into a SC, so the user could install the sensor systems of their cupboard without needing to replace their original cupboard.

In the early detection of diseases, it can be difficult to sell products to healthy people, even if the product is cheap. We argue that as in the case of many other successful smart devices in the market (e.g., smartphones, smartbands, and smart TVs), SCs could have multi-purpose functionalities for successfully getting to the market. In this line, the SC could also be useful for detecting eating patterns by classifying different kinds of food in different compartments. Eating patterns can be useful for controlling dietary habits to reduce obesity, which is an issue for many people in countries like the US [22]. Eating patterns could also be useful for tracking emotions by considering their known relationship [23].

The experiments showed that the reaction time measured by the SC test did not correlate with the reaction of the control test about face–name pairs. However, these results are not conclusive, since the number of participants ($n = 23$) was not sufficient to detect medium effect sizes according to the analysis based on statistical power performed by the G*Power 3 tool [24]. In addition, not all memory tests need to have a correlation between reaction time and memory. In fact, strictly a memory test needs to provide some measure that correlates with memory, which could be either accuracy or reaction time, but not necessarily both. Thus, the proposed SC test is a reliable memory test according to the common standards of memory tests [25].

In addition, the accuracy of the SC memory test correlated with self-perceived memory, even though the literature supports that self-perceived memory is influenced by factors such as personality [20], which could lead to differences between self-perceived memory and actual memory.

One limitation of the current version of the SC is that it is based on the assumption that there is only one person using the SC to reliably measure their memory. We plan to overcome this limitation by including an identification mechanism, which could either be (1) facial identification with a low-cost camera following our previous work in facial authentication [26] or (2) radio-frequency identification, which would require the user to carry a card for the identification. We will select one of these options considering economic aspects, technological reliability, and user experience. In this manner, the SC will determine who is using it and perform different measurements for the different family members. In general, the inclusion of identification will allow engineers to develop SC applications for providing customized services to the user.

In the future, we plan to conduct a study with Alzheimer's patients over a 10-month period to detect memory losses during the evolution of this disease, by measuring the memory of the same persons through the study with the proposed SC-based approach. If possible, we will also enroll people considered to probably start having Alzheimer's disease soon, known by the analysis of genetic information in descendants of people with Alzheimer's. As a control group, we also plan to track the memory evolution of a group of healthy people, which may include some of the participants of the presented study. In this way, we plan to detect improvement opportunities and further assess whether it is possible to track memory losses and to detect Alzheimer's at an early stage.

Another future work is the development of an app whose main aim will be to explain to users how to turn a normal cupboard into an SC using gamification to overcome the barrier of a possible difficult installation. Finally, our efforts will focus on improvement of energy efficiency, since cupboards are not used very frequently. This could be achieved by lowering the checking frequency of sensors when users do not usually use them, based on an initial training phase, following a similar approach to our previous one in green communications with smartbands [27]. Another option that involves the power system is to use some energy-harvesting techniques to overcome the limitation of the long-term use of the SC powered by batteries. The aim of harvesting techniques is to accumulate energy from several sources that capture energy from the environment. Once the energy is accumulated, it can be used in the SC to track user memory. Several examples of energy harvesting can be found in the literature [28], but techniques that involve components such as micro-photovoltaic cells, micro-thermoelectric generators [29], or indoor ambient light [30] may be the most suitable for SCs. Furthermore, we also plan to develop an app for remotely consulting memory measurement results from any mobile device, and to provide notifications if a family member is starting to have significant memory losses.

Author Contributions: Conceptualization, F.G.-L., I.G.-M. and R.A.; Data curation, F.G.-L. and I.G.-M.; Formal analysis, F.G.-L. and I.G.-M.; Funding acquisition, I.G.-M. and R.L.; Investigation, F.G.-L., I.G.-M., R.A. and R.L.; Methodology, F.G.-L., I.G.-M., R.A. and R.L.; Project administration, I.G.-M.; Software, F.G.-L.; Supervision, I.G.-M., R.A. and R.L.

Funding: This work was mainly devised during the research stay of the second author in the Massachusetts General Hospital and Harvard University, funded by "Dpto. de Innovación, Investigación y Universidad del Gobierno de Aragón" through the program "FEDER Aragón 2014-2020 Construyendo Europa desde Aragón" (Ref: T49_17R). This work has also been financed by the Aragonese Government and the UE through the FEDER 2014–2020 "Construyendo Europa desde Aragón" action (Group T25_17D). We also acknowledge the support of the projects "Collaborative Ambient Assisted living Design" (TIN2014-57028-R), "Diseño colaborativo para la promoción del bienestar en ciudades inteligentes inclusivas" (TIN2017-88327-R), and "Red Temática de Investigación en Ciudades Inteligentes" (TIN2016-81766-REDT) funded by the Spanish council of Science, Innovation and Universities from the Spanish Government.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

GPIO	General-Purposes Input/Output
I2C	Inter-Integrated Circuit
ID	Identifier
IoT	Internet of Things
M2M	Machine-to-Machine
SD	Standard Deviation
SPI	Serial Peripheral Interface
SC	Smart Cupboard
TV	Television
UART	Universal Asynchronous Receiver-Transmitter
US	United States

References

1. Prince, M.; Comas-Herrera, A.; Knapp, M.; Guerchet, M.; Karagiannidou, M. *World Alzheimer Report 2016: Improving Healthcare for People Living with Dementia: Coverage, Quality and Costs Now and in the Future*; Alzheimer's Disease International (ADI): London, UK, 2016.
2. Roopaei, M.; Rad, P.; Prevost, J.J. A Wearable IoT with Complex Artificial Perception Embedding for Alzheimer Patients. In Proceedings of the 2018 World Automation Congress (WAC), Stevenson, WA, USA, 3–6 June 2018; pp. 1–6.
3. Birks, J.S.; Harvey, R.J. Donepezil for dementia due to Alzheimer's disease. *Cochrane Database Syst. Rev.* **2018**, *6*. [[CrossRef](#)] [[PubMed](#)]
4. Chang, C.H.; Lane, H.Y.; Lin, C.H. Brain Stimulation in Alzheimer's Disease. *Front. Psychiatry* **2018**, *9*, 201. [[CrossRef](#)] [[PubMed](#)]
5. Prince, M.; Bryce, R.; Albanese, E.; Wimo, A.; Ribeiro, W.; Ferri, C.P. The global prevalence of dementia: A systematic review and metaanalysis. *Alzheimers Dementia* **2013**, *9*, 63–75. [[CrossRef](#)] [[PubMed](#)]
6. Kortuem, G.; Kawsar, F.; Sundramoorthy, V.; Fitton, D. Smart objects as building blocks for the internet of things. *IEEE Internet Comput.* **2010**, *14*, 44–51. [[CrossRef](#)]
7. García-Magariño, I.; González-Landero, F.; Amariglio, R.; Lloret, J. Collaboration of Smart IoT Devices Exemplified With Smart Cupboards. *IEEE Access* **2019**, *7*, 9881–9892. [[CrossRef](#)]
8. Nonavinakere, S.; Aldana, J.; Sisson, S.; Cruz, E.; George, K. Memory Aid Device to Improve Face-Name Memory in Individuals with Alzheimer's Disease. In Proceedings of the 2018 IEEE International Conference on Healthcare Informatics (ICHI), New York, NY, USA, 4–7 June 2018; pp. 353–354.
9. Crema, C.; Depari, A.; Flammini, A.; Sisinni, E.; Benussi, A.; Borroni, B.; Padovani, A. Embedded platform-based system for early detection of Alzheimer disease through transcranial magnetic stimulation. In Proceedings of the 2018 IEEE Sensors Applications Symposium (SAS), Seoul, Korea, 12–14 March 2018.
10. Narendiran, A.; Nandan, M.M.; Naveen, B. Cognitive Assistance in Smart Homes to Model the Progression of Alzheimer Disease. *J. Adv. Res. Appl. Sci.* **2018**, *5*, 149–163.
11. Ishii, H.; Kimino, K.; Aljehani, M.; Ohe, N.; Inoue, M. An early detection system for dementia using the M2 M/IoT platform. *Procedia Comput. Sci.* **2016**, *96*, 1332–1340. [[CrossRef](#)]
12. Kristalina, P.; Imanuddin, A.I.; Yuliana, M.; Pratiarso, A.; Astawa, I.G.P. Alzheimer Patient Tracking System in Indoor Wireless Environment. *European Scientific Journal, ESJ* **2017**, *13*, 327. Available online: <http://ejournal.org/index.php/esj/article/view/10194> (accessed on 3 June 2019). [[CrossRef](#)]
13. Chavan, S.C.; Chavan, A. Smart wearable system for fall detection in elderly people using internet of things platform. In Proceedings of the 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 15–16 June 2017; pp. 1135–1140.
14. Paul, M.C.; Sarkar, S.; Rahman, M.M.; Reza, S.M.; Kaiser, M.S. Low cost and portable patient monitoring system for e-Health services in Bangladesh. In Proceedings of the 2016 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 7–9 January 2016.

15. Chong, Z.H.K.; Tee, Y.X.; TOH, L.J.; Phang, S.J.; Liew, J.Y.; Queck, B.; Gottipati, S. Predicting potential Alzheimer medical condition in elderly using IOT sensors-Case study. In Proceedings of the IRC Conference on Science, Engineering, and Technology, Singapore, 10–11 August 2017. Available online: https://ink.library.smu.edu.sg/sis_research/3834/ (accessed on 3 June 2019).
16. Navarro, J.; Doctor, F.; Zamudio, V.; Iqbal, R.; Sangaiyah, A.K.; Lino, C. Fuzzy adaptive cognitive stimulation therapy generation for Alzheimer’s sufferers: Towards a pervasive dementia care monitoring platform. *Future Gener. Comput. Syst.* **2018**, *88*, 479–490. [[CrossRef](#)]
17. Hampstead, B.M.; Sathian, K.; Moore, A.B.; Nalisnick, C.; Stringer, A.Y. Explicit memory training leads to improved memory for face–name pairs in patients with mild cognitive impairment: Results of a pilot investigation. *J. Int. Neuropsychol. Soc.* **2008**, *14*, 883–889. [[CrossRef](#)] [[PubMed](#)]
18. Hamrick, P. Declarative and procedural memory abilities as individual differences in incidental language learning. *Learn. Individ. Differ.* **2015**, *44*, 9–15. [[CrossRef](#)]
19. Tak, S.H.; Hong, S.H. Face-name memory in Alzheimer’s disease. *Geriatr. Nurs.* **2014**, *35*, 290–294. [[CrossRef](#)] [[PubMed](#)]
20. Buchanan, T. Self-assessments of memory correlate with neuroticism and conscientiousness, not memory span performance. *Pers. Individ. Differ.* **2017**, *105*, 19–23. [[CrossRef](#)]
21. Benesty, J.; Chen, J.; Huang, Y.; Cohen, I. Pearson correlation coefficient. In *Noise Reduction in Speech Processing*; Springer: New York, NY, USA, 2009.
22. Flegal, K.M.; Carroll, M.D.; Ogden, C.L.; Curtin, L.R. Prevalence and trends in obesity among US adults, 1999–2008. *JAMA* **2010**, *303*, 235–241. [[CrossRef](#)] [[PubMed](#)]
23. Macht, M.; Simons, G. Emotions and eating in everyday life. *Appetite* **2000**, *35*, 65–71. [[CrossRef](#)] [[PubMed](#)]
24. Faul, F.; Erdfelder, E.; Lang, A.G.; Buchner, A. G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behav. Res. Methods* **2007**, *39*, 175–191. [[CrossRef](#)] [[PubMed](#)]
25. Ross, S.; Krukowski, R.; Putnam, S.; Adams, K. The Memory Assessment Scales in the detection of incomplete effort in mild head injury. *Clin. Neuropsychol.* **2003**, *17*, 581–591. [[CrossRef](#)] [[PubMed](#)]
26. Guillén-Gámez, F.D.; García-Magariño, I.; Bravo-Agapito, J.; Lacuesta, R.; Lloret, J. A proposal to improve the authentication process in m-health environments. *IEEE Access* **2017**, *5*, 22530–22544. [[CrossRef](#)]
27. González-Landero, F.; García-Magariño, I.; Lacuesta, R.; Lloret, J. Green communication for tracking heart rate with smartbands. *Sensors* **2018**, *18*, 2652. [[CrossRef](#)] [[PubMed](#)]
28. Huang, Q.; Lu, C.; Shaurette, M. Feasibility study of indoor light energy harvesting for intelligent building environment management. In Proceedings of the International High Performance Buildings Conference, West Lafayette, IN, USA, 12–15 July 2010. Available online: <https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1017&context=ihpbc> (accessed on 3 June 2019).
29. Huang, Q.; Lu, C.; Shaurette, M.; Cox, R. Environmental thermal energy scavenging powered wireless sensor network for building monitoring. In Proceedings of the 28th International Symposium on Automation and Robotics in Construction, Seoul, Korea, 29 June–2 July 2011; pp. 1376–1380.
30. Lu, C.; Raghunathan, V.; Roy, K. Efficient design of micro-scale energy harvesting systems. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2011**, *1*, 254–266. [[CrossRef](#)]



6.3. PriorityNet App: A mobile application for establishing priorities in the context of 5G ultra-dense networks.

Cita completa:

GONZÁLEZ-LANDERO, F., GARCÍA-MAGARIÑO, I., LACUESTA, R., & LLORET, J. (2018). PriorityNet App: A mobile application for establishing priorities in the context of 5G ultra-dense networks. *IEEE Access*, 614141-14150.

Abstract:

The devices and implementations of 5G networks are continuously improving, and people will probably use them daily in the near future. 5G networks will support ultra-dense networks. In the literature, several works apply 5G networks in smart cities and smart houses. One of the most common features of these works is to use priorities in tasks, such as the management of electrical consumption at houses, waste collection in cities, or pathfinding in self-driving cars. The proper management of priorities facilitates that urgent service requests are rapidly attended. However, to the best of our knowledge, the literature lacks appropriate mechanisms for considering users' priorities in the 5G ultra-dense networks. In this context, we propose a mobile application that allows citizens to request smart city services with different priority levels. The experiments showed the high performance of the app and its scalability when increasing priority list sizes. This app obtained 72.3% of usability in the system usability scale and 82.9% in the ease-of-use dimension of the usefulness, satisfaction, and ease of use questionnaire.

Received January 23, 2018, accepted February 24, 2018, date of publication March 5, 2018, date of current version March 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2811900

PriorityNet App: A Mobile Application for Establishing Priorities in the Context of 5G Ultra-Dense Networks

FRANKS GONZÁLEZ-LANDERO¹, IVÁN GARCÍA-MAGARIÑO^{2,3},
RAQUEL LACUESTA^{2,3}, (Member, IEEE), AND JAIME LLORET⁴, (Senior Member, IEEE)

¹Edison Desarrollos, 44002 Teruel, Spain

²Department of Computer Science and Engineering of Systems, University of Zaragoza, 44003 Teruel, Spain

³Instituto de Investigación Sanitaria Aragón, 50009 Zaragoza, Spain

⁴Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politècnica de Valencia, 46022 Valencia, Spain

Corresponding author: Jaime Lloret (jlloret@dcom.upv.es)

This work was supported in part by the Construcción de un framework para agilizar el desarrollo de aplicaciones móviles en el ámbito de la salud through the University of Zaragoza and the Fundación Ibercaja under Grant JIUZ-2017-TEC-03, in part by the Program—Estancias de movilidad en el extranjero José Castillejo para jóvenes doctores through the Spanish Ministry of Education, Culture and Sport under Grant CAS17/00005, in part by the Universidad de Zaragoza, Fundación Bancaria Ibercaja, and Fundación CAI in the Programa Ibercaja-CAI de Estancias de Investigación under Grant IT24/16 and Grant IT1/18, in part by the Research Project—Desarrollo Colaborativo de Soluciones AAL through the Spanish Ministry of Economy and Competitiveness under Grant TIN2014-57028-R, in part by the Organismo Autónomo Programas Educativos Europeos under Grant 2013-1-CZ1-GRU06-14277, in part by the Fondo Social Europeo and the Departamento de Tecnología y Universidad del Gobierno de Aragón under Grant Ref-T81, and in part by the Ministerio de Economía y Competitividad in the Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento within the project under Grant TIN2017-84802-C2-1-P.

ABSTRACT The devices and implementations of 5G networks are continuously improving, and people will probably use them daily in the near future. 5G networks will support ultra-dense networks. In the literature, several works apply 5G networks in smart cities and smart houses. One of the most common features of these works is to use priorities in tasks, such as the management of electrical consumption at houses, waste collection in cities, or pathfinding in self-driving cars. The proper management of priorities facilitates that urgent service requests are rapidly attended. However, to the best of our knowledge, the literature lacks appropriate mechanisms for considering users' priorities in the 5G ultra-dense networks. In this context, we propose a mobile application that allows citizens to request smart city services with different priority levels. The experiments showed the high performance of the app and its scalability when increasing priority list sizes. This app obtained 72.3% of usability in the system usability scale and 82.9% in the ease-of-use dimension of the usefulness, satisfaction, and ease of use questionnaire.

INDEX TERMS Smart city, priority, ultra-dense network, mobile application, app.

I. INTRODUCTION

Nowadays each citizen commonly has a mobile device. The amount of interchanged information usually increases due to the active use of clouds, document repositories and streaming-video servers. It is predicted that the number of connected mobile devices will exceed 11.5 billion in 2019. In addition, 5G ultra-dense networks [1] will probably efficiently support all these connections, especially in smart cities with a high population density.

5G technologies are advancing in several aspects such as (a) the reduction of energy consumption, (b) the improvement of signal reachability in wall trespassing [2], and (c) the

management of networks for rapidly transferring big data. The demand of data traffic is increasing steeply for transferring large files such as high-resolution videos, which have up-growing popularity [3]. In this line of work, a software-defined networking (SDN) approach improved the fairness in streaming video so that users get this service with a similar quality level [4]. In addition, an intelligent handover process algorithm guaranteed load balance in 5G networks, and improved the quality of service (QoS) in the upload of videos from mobile cameras in environmental surveillance [5]. 5G networks are also useful in fields that need real-time responses such as e-health monitoring [6]. In general,

5G networks are based in some pillars such as SDN, network function virtualization (NFV) and mobile edge computing (MEC) [7].

Smart cities need to urgently attend some service requests, such as waste collection in some critical locations like hospitals, chemical factories and schools [8].

Our previous work shows that priorities self-reported by citizens can be fairly managed even when there are people trying to take advantage of the priority system [9]. However, in order to allow citizens to easily self-report the priority levels of their requests, an easy-to-use app could be useful for final users. This work addresses this problem by proposing a novel app that allow users to define their prioritized lists of service requests.

The remainder of the paper is organized as follows. The next section introduces the related work, highlighting the gaps of the literature that the current work addresses. Section III presents the current approach introducing the novel PriorityNet app. Section IV describes the experiments about the performance and usability of the app. Finally, section V mentions the conclusions, and depicts some future lines of research.

II. RELATED WORK

The most relevant related works fall into the three categories of (a) smart cities with their communications and smart services discussed in II-A, (b) solutions for supporting ultra-dense networks introduced in section II-B, and (c) applications that manage priorities for tasks or services presented in section III-C.

A. SMART CITIES

Smart cities usually need to communicate large amounts of data. Some of the smart city services are real time, and need short latencies. Hence, an adequate networking performance generally has a positive effect on the citizens quality of life.

To begin with, [8] proposed four dynamic models for collecting waste in smart citizens. In summary, a smart city had a fleet of trucks and several trash bins. Each bin had a device for tracking when it was full. The models distinguished between two types of bins, which were the high priority bins (HPBs) and the other ones. The HPBs were located in places such as hospitals, factories and high schools. The models were the Dedicated Trucks Model (DTM), Detour Model (DM), the Minimum Distance Model (MDM) and the Reassignment Model (RM). They described how trucks collected waste from HPBs in each model. Each model has its mechanism of reassigning routes. They evaluated the models in Saint Petersburg (Russia), and all of them had advantages and disadvantages. A set of simulations showed the utility of their approach and the proper functioning of the route reassignment mechanisms. They mentioned the possibility of expanding their work by taking truck capacities into account. However, this work did not allow users to change the priorities of certain bins. For example, this could be useful for requesting the collection of a really risky material,

like an extraordinarily highly toxic waste from a chemical factory.

Moreover, [10] introduced some of the smart city bases such as 5G networks, Internet of Things (IoT), cloud of things and advanced artificial intelligence. Smart cities normally had smart homes. 5G technologies were used for two purposes. The first one was to let people communicate with their smart homes. For example, they could use their mobile devices for remotely scheduling the tasks of IoT appliances. The second purpose was to facilitate the transfer of huge amounts of data with clouds. In the future, it will be necessary to have more bandwidth for performing such operations. Lastly, smart cities were expected to collect information from citizens in order to take better decisions for improving their quality of life. For instance, a smart city could analyze electrical consumption in each house, and provide customized recommendations for saving money. More concretely, similar approaches can be adopted to specific buildings. For example, [11] presented a case study about products for improving security in smart buildings. In smart homes, this work used surveillance devices such as motion detector, sensors for opening/closing doors, and presence sensors. All of these were connected to Internet so that users could check their homes with their mobile devices. Nevertheless, none of these works proposed an app for establishing priorities for most urgent matters. In the case of surveillance, the transmission of some cameras may need a higher priority in some situations such as robberies.

Furthermore, [12] presented a theoretical model about self-driving connected cars. This model was based on the theory of multi-agent system. Each vehicle was represented as an individual agent in simulations. They followed a Belief-Desire-Intention (BDI) approach [13], in which each agent was aimed at satisfying its desires by completing some specific goals. The connected cars were an innovative solution for reducing collision risk, avoiding economic cost of crashes and saving humans lives. Furthermore, disabled people, elders or people without valid driver's license could safely travel long distances. Moreover, vehicle-to-vehicle (V2V) communication were necessary for supporting this self-driving model. Thanks to V2V communications, cars could potentially exchange information about their positions, speeds, routes, plans for changing speed or lane, turning, stopping and so on. This model was simulated with Qt Framework 5.4, and it worked properly. However, this model would need to consider more aspects to be applied in real world, such as the possibility that large amounts of messages could overload V2V networks and the limitations of the city infrastructures. Hence, 5G networks could be useful for efficiently transferring these amounts of data avoiding losses. Nonetheless, this work did not mention the possibility of establishing priorities for assuring the safe travel in self-driving cars. A proper mechanism of prioritization could overcome this barrier. For example, the communications of some cars could be prioritized when transporting patients in critical health situations.

Therefore, in most of these works, an app could be useful for allowing users to manually change the priorities in some services in real time.

B. ULTRA-DENSE NETWORKS

In the current society, the use of mobile device connections is increasing rapidly. In this context, the field of ultra-dense networks is aimed at supporting dense sets of connection points. Several works have discussed new technological advances in ultra-dense networks. For instance, [2] introduced the variety of 5G technologies with cognitive radio (CR). CR is a mechanism for dynamically selecting the best wireless channels according to different criteria for avoiding congestions and interferences. They addressed the challenge of saving energy in smart home networks (SHNs), considering the spread of WiFi signal. [14] mentioned that devices needed a high amount of energy to emit signals for communications through obstacles. CR was planned to be implemented with 5G technologies. They made a simulation of a SHN with and without CR, and the energy consumption was reduced in 26%.

Several works about ultra-dense networks focus on transferring files with large amounts of data. For example, [15] proposed a new framework that was able to support huge data traffics requested by users. This framework was called Big Data Driven. It focused on providing a high quality of experience to users with their mobile devices and wearable sensors. Basically this model reallocated resources to manage data traffic based on the user locations. Moreover, this framework also reduced some costs by analyzing data from users. In addition, [3] presented a new paradigm called Information-centric-networking (ICN). This paradigm was aimed at retrieving videos from in-network caches. ICN reduced network traffic and video retrieval delay significantly. However, these kinds of applications may have a low priority when sharing the network with other more critical services (e.g. critical health situations and network failures).

Reference [16] proposed a mechanism for improving communications among neighbor cells. It was based on a reward mechanism for promoting collaboration. Their approach considered real-time priority levels and QoS.

In conclusion, ultra-dense networks usually need intensive transfer of data. Some services may need urgent responses. These urgencies can dynamically vary depending many factors. An easy-to-use app could be useful to allow users to indicate these changing priorities in smart cities.

C. PRIORITY APPLICATIONS

The priorities of services and tasks have been widely used in many fields. For instance, [17] proposed a cultivation priority planning based on the needs of food and the locations provided by a geographical information system (GIS). Their approach considered several aspects such as soil depth, climate, pH, and the existence of certain minerals in the land. They applied a fuzzy approach and an analytical hierarchy

process to assign the cultivation type to the different land areas.

Moreover, in the field of parallel computing, [18] proposed to use user-assigned priorities for job scheduling. Their approach was based on their ReShape framework that supported resizing parallel applications. The priorities were used to take informed decisions about changing the number of processors assigned to each job. They applied their framework in three case studies, and they obtained improvements of the execution time and higher utilization of the existing resources.

In the public transportation area, [19] used several flexible priority rules for assigning passengers to trains and seats. Their approach had low computational times. They did not significantly increase the level of unattended requests or travel delays. However, they increased the variability of passengers. In this manner railway operators were able to test different policies about passenger priorities.

The Priority-based Application-Specific Congestion Control Clustering protocol (PASCOC) [20] used priorities for managing network communications. PASCOC used a clustering approach for detecting congestions in the network and avoiding these areas. Some of the communications needed to take larger paths in networks for avoiding congestions. The priorities were used to select which communications used the shorter paths and which ones the larger ones. In addition, [21] proposed to use priorities for managing services through sensor networks in general.

Nevertheless, none of these works explicitly provided an easy-to-use mobile application for allowing final users to establish their own priorities. The next section introduces a novel app that covers this gap of the literature.

III. PRIORITYNET: AN APP FOR SETTING PRIORITIES IN ULTRA-DENSE NETWORKS

PriorityNet app is a tool that allows users to easily assign priorities to certain service requests. This tool was developed considering usability principles.

Figure 1 depicts the functionality of the app and some of its possible utilities. Users can determine priority lists for themselves or companies. The app connects with the system and uploads these priority lists. In this way, a user could set the priorities in several service requests of a smart home, such as the ones related with security cameras (e.g. when something suspicious had been observed), turning on/off electrical appliances, or download video streaming in real time with a high quality. In smart cities, the priorities could be used for reassigning routes in self-driving cars or trucks that collect dangerous waste.

A. USER INTERFACE

Figure 2 presents the main screen of the app, which allows users to define priority lists. This screen has two vertical lists. The list in the right side contains certain services, including the ones from the smart city or the use of the network for certain mobile applications. Priorities can be assigned for all

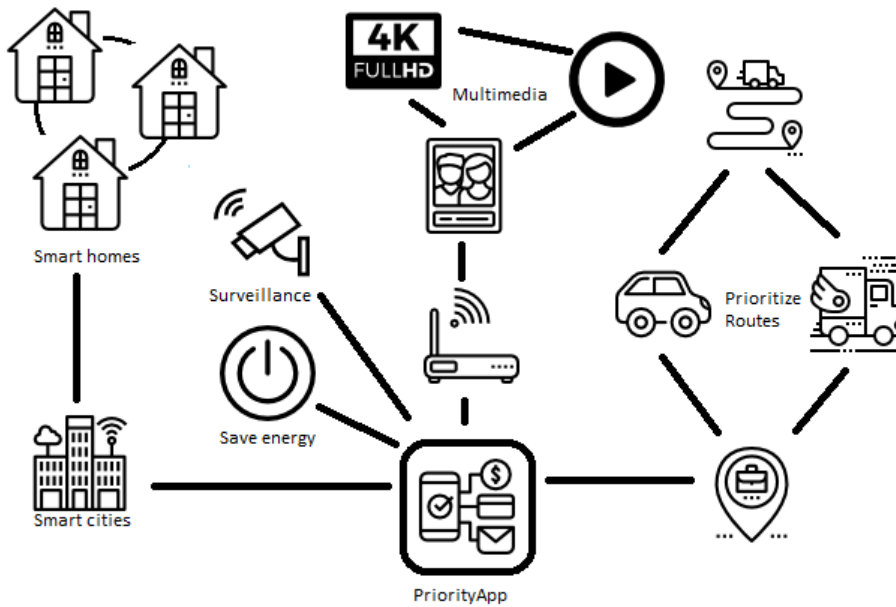


FIGURE 1. Overview of the priority system of PriorityNet app.



FIGURE 2. Main screen of PriorityNet App.

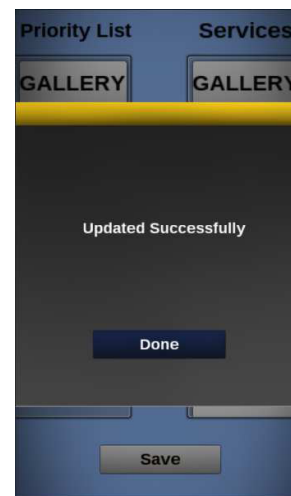


FIGURE 3. Confirmation message in PriorityNet app.

these services and mobile applications. The priority order is established in the left list by dragging and dropping elements from the right-side list. The services with more priority are placed at the top of the list and the ones with less priority are placed at its bottom.

The use of this application is summarized in three steps. In the first step, the user decides the service to which they assign higher priorities. In the second step, the user drags and drops an item from the right list to the left one. In the last step, the user can re-sort the the priorities of the list of services, if they want to.

When a user has finished assigning priorities to services, they can touch the “Save” button, and the priority list is transferred to the system. Figure 3 shows an example of a confirmation message.

B. DESIGN AND IMPLEMENTATION

As one can observe in the sequence diagram of Figure 4, users can see all available services. In this step, they must drag one service and drop it in a priority list, so that this priority list is created. The sequence diagram has a squared yellow background in order to indicate that this operation part continues as long as the user wants. Hence, it is possible to rearrange priorities, and adding/deleting services to/from the list.

When the user touches the 'Save' button, the system receives input from the priority list, converts it into a JavaScript Object Notation (JSON) file, and sends it to a database management system (DBMS). JSON is a file format for sending information to DBMSs. The DBMS can be running either in a cloud or a specific server. The server has

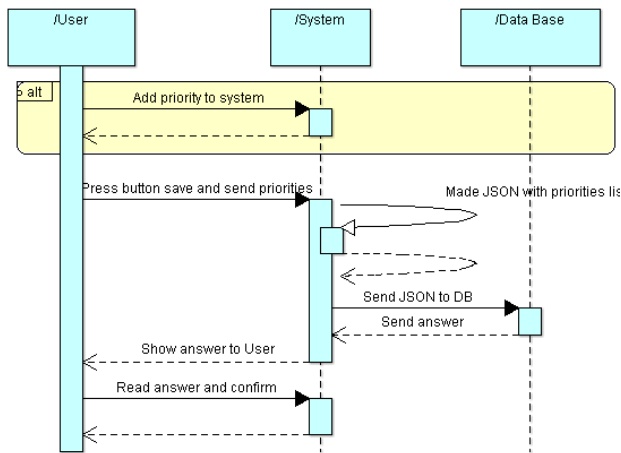


FIGURE 4. Sequence diagram for creating and saving a priority list.

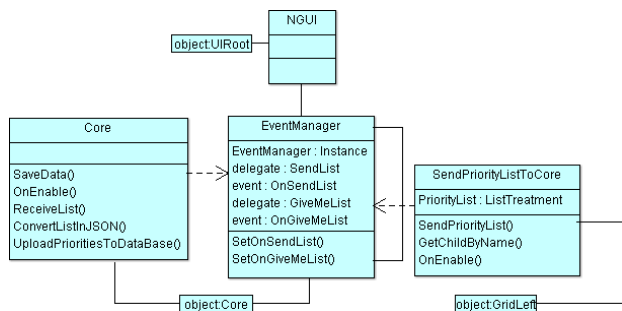


FIGURE 5. Class diagram excerpt of PriorityNet app.

several scripts in PHP programming language. One of these receives information from a JSON file.

PriorityNet app sends information to DBMS through a web request, specifically a POST request. The request includes the JSON file content, and the URI/URL of the receptor script for managing the information. When a PHP file receives a request, it might update, add or delete information depending on the content of the JSON file. In case of managing a change of priority list in the network, the PHP file updates the database with a new priority list for a specific user. Finally, the PHP file returns another JSON file to the mobile device. This JSON file contains information about the result of the query in the DBMS, which can be either a confirmation of success or an error. In this way, users can read this message, and could repeat their actions later if necessary.

The class diagram of Figure 5 specifies the structure of two classes. On the one hand, the “Core” class receives input from a priority list, turns it into a JSON file, and uploads the converted file to the DBMS. On the other hand, the “EventManager” class receives input from a list of events and delegates, and was implemented with a singleton pattern. A delegate is a type that represents references to methods with a particular parameter list and a return type. Events are triggered for notifying some observers when something of interest occurs. The methods of some classes are associated with these events.

The “SendPriorityListToCore” class has a method that collects all the items from the priority list, and sends the names of these items as strings to the Core class. After executing this method, the system collects this priority list, and adds certain information for conforming a JSON file. This file includes information such as the user ID. This ID allows the system to track users and to manage priorities fairly.

PriorityNet App was developed with Unity 3D engine and the library Next Graphical User Interface (NGUI) [22]. Unity 3D has been widely used in both industry and research communities, like in the simulation of distributed sensor networks [23]. One of its main advantage is its multi-platform nature, allowing the deployment of apps in the main mobile operative systems such as Android and iOS. We used NGUI for performing tasks associated with the user interface. The NGUI library was created by Tasharen Entertainment and released in 2011. The main aim of NGUI was to ease the creation of user interfaces. In the presented app, NGUI was useful for adding the drag and drop functionality. NGUI also supported the implementation of lists with draggable elements. These functionalities were relevant for achieving an easy-to-use and intuitive app.

C. PRIORITY MECHANISM

The priority mechanism of the current approach is aimed at satisfying the following rule in which the differences of waiting times should be as large as possible:

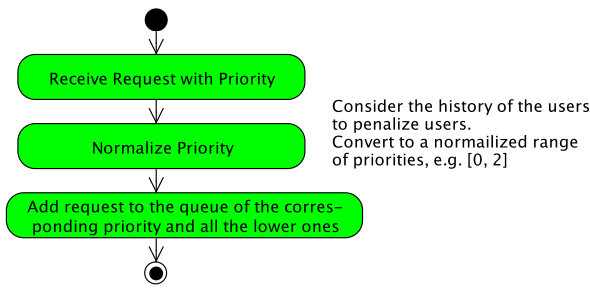
$$p(r_x) > p(r_y) \Rightarrow w(t_x) \geq w(t_y) \tag{1}$$

where r_x and r_y are requests of services, $p(r)$ determines the priority of r request, and $w(r)$ determines its waiting time.

Figure 6 shows the block diagram of the mechanism for managing and attending requests. On the one hand, the system manages the reception of requests of smart city services, as shown in the left side of the diagram. The system receives a request with a certain priority. Then, the system normalizes this priority into the range of priorities of the system, e.g. [0, 2] being zero the highest priority and two the lowest one. In this step, the system can optionally use a mechanism of normalizing the priorities to avoid selfish citizens. The system has several queues of requests, and each queue is associated with the requests of each priority level. In order to attend the high-priority requests first, the requests are not only added to the queue of its level but also to the ones with lower priority levels. In this manner, it is guaranteed that each request is attended before any other later request of its level or lower ones.

On the other hand, this priority mechanism attends the service requests in each iteration, as one can observe in the right side of Figure 6. It starts with the highest-priority queue. In order to regulate that normally high priorities are attended much faster, the number of attended requests per iteration is different for each queue regarding its priority level. For example, in each iteration, the system can attend three requests of the highest priority level, two requests of the medium priority level and one priority of the lowest iteration level. Once a

System manages the reception of requests



System attends requests

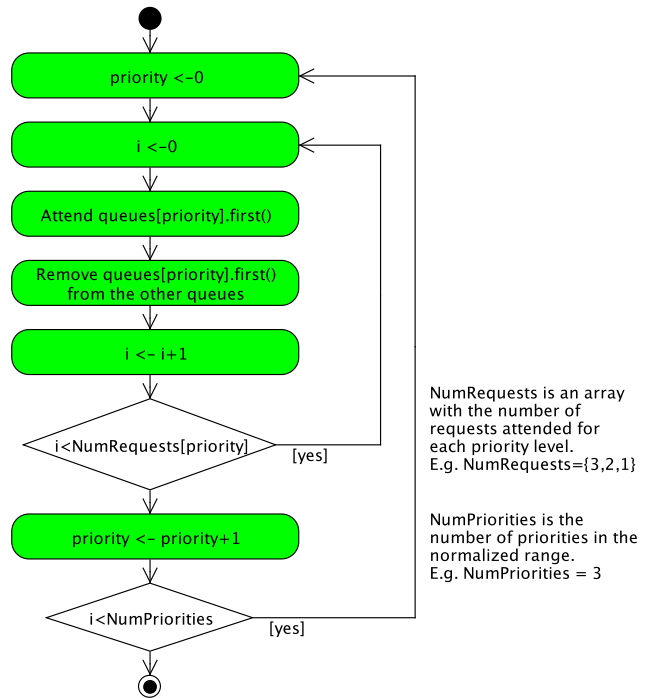


FIGURE 6. Block diagram of the priority mechanism.

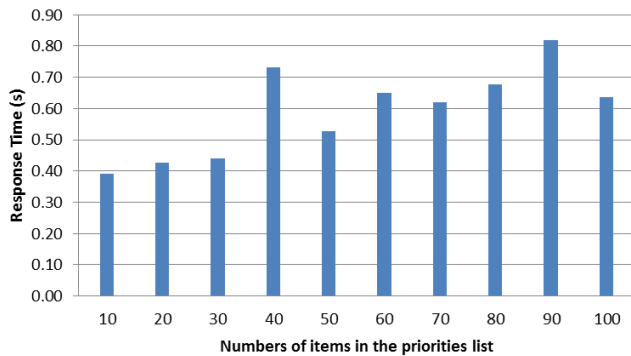


FIGURE 7. Response time of PriorityNet App.

request is attended, it is removed from the corresponding queue and all the others.

IV. EXPERIMENTATION

A. EVALUATION OF RESPONSE TIME

We measured the response time of PriorityNet when uploading a priority list to the system. This task includes (a) converting a priority list into a JSON file, (b) sending a POST request with a JSON file, (c) receiving an answer from the server, and (d) processing the server’s answer. We measured all the time elapsed between touching the Save button and the presentation of the confirmation message to the user.

These experiments used lists of sizes from 10 to 100 with intervals of ten. We performed 100 executions for each list size, and Figure 7 presents the average results.

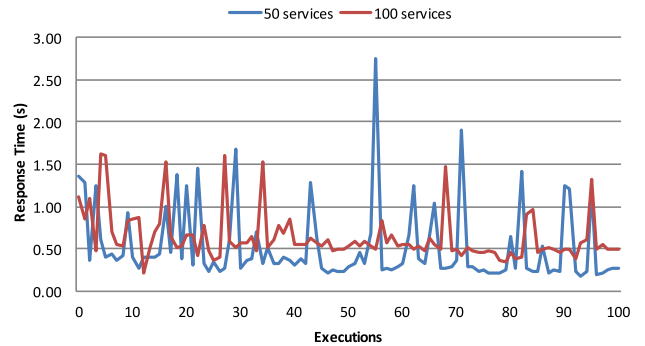


FIGURE 8. Response times for uploading priority lists of respectively 50 and 100 services.

As one can appreciate, the average time never exceeded one second in any case. We consider these results as satisfactory, because the user did not wait an excessive time even when using priority lists of 100 services.

The experimentation with PriorityNet showed its scalability. When increasing the size of the priority list, the response time only slightly increased. There were some exceptions in the results collected from priority lists of sizes 40 and 60.

Moreover, Figure 8 shows all the response times for uploading priority lists of respectively 50 and 100 services. We executed 100 times the upload process for each of these two list sizes. Both priority list sizes had some peaks that are high in comparison to their common values. These peaks may be due external factors regarding the network, such as congestions or general overloads.

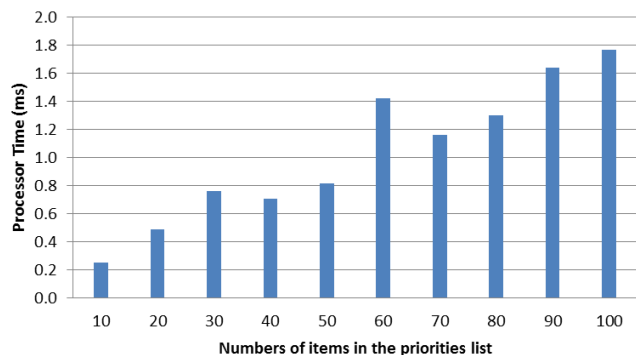


FIGURE 9. Processing time of PriorityNet app.

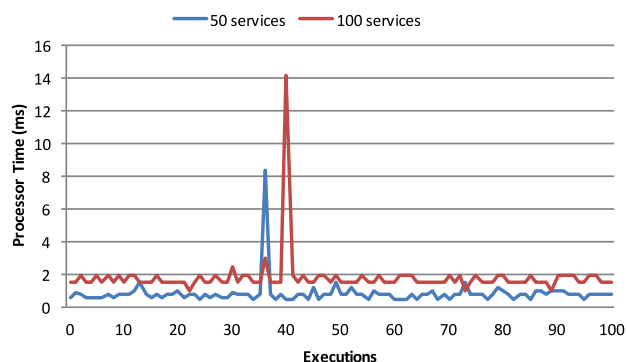


FIGURE 10. Processing times for lists of respectively 50 and 100 services.

B. EVALUATION OF PROCESSING TIME

We measured the processing time of PriorityNet app when defining and saving priority lists. More concretely, we measured the elapsed time from pressing the Save button until the data were prepared to be transferred. This includes (a) triggering an event to request the priority list, (b) receiving a priority list by means of a delegate, and (c) converting the visual list into a serializable format.

This analysis executed 100 times each of the same ten priority list sizes as before. Figure 9 shows the average results of the processing time for these list sizes. It is worth noting that the absolute values of processing time were low. For example, the average processing time for priority lists of 100 services was only 1.76 ms.

Figure 10 shows the processing times of 100 executions for priority list sizes of respectively 50 and 100 services. Most values of each priority list size were near its corresponding average, which was 0.81 ms for lists of 50 services and 1.76 ms for lists of 100 services. There was a high peek value for each priority list size, but we consider that these values are outlier, since they only occurred once in each analyzed set of 100 simulations. The standard deviation values of 0.78 ms (for the list of 50 services) and 1.28 ms (for the list of 100 services) revealed that the variation of processing times was low considering their absolute values.

C. USER STUDY

We conducted a user study to measure some features of the users’ experience when using PriorityNet app.

TABLE 1. Priority lists for the tests of the user study.

Test 1	Test 2	Test 3
Music	Send Message	Maps
Maps	Calendar	Clock
Whatsapp	Music	Radio
Gallery	E-mail	Send Message
Radio		GPS
Send Message		

1) SAMPLE OF PARTICIPANTS

We recruited 21 people for participating in this user study. They were 21.1 years old in average (SD=4.17). Seven participants were male (33.3%) and the others were female (66.6%). Only one participant worked or studied in computer science field (0.047%).

2) PROCEDURE

The app was briefly introduced to each participant. Then, the experimenter briefly showed how to use the app to each participant. More concretely, he explained how to set up priorities in the system. Participants saw how to drag and drop items from the right list to left one, and they only saw this operation. The experimenter did not explain how to alter the elements of the priority list if they had made a mistake, either including the wrong element or assigning it to the wrong priority. We did not explain this on purpose, because if the app was sufficiently easy to use, users should be able to deduce it by themselves.

The experimenter asked each participant to sequentially define and save the priority lists presented in table 1. The first priority list was longer than the others to let them get used to the app. The second list had items that the users were not able to see without scrolling down. In this way, participants needed to scroll down for completing the task. The last test was similar to the second one. The main difference was the way to do it. When a participant had finished a test, this participant was told to change the order of the items of the list.

Lastly, the participants were asked to answer a questionnaire about this application. This questionnaire was composed from the validated scales mentioned in next section.

3) MEASURES

The questionnaire about the app was composed of several validated scales. The first scale was the System Usability Scale (SUS) [24]. SUS is composed of 10 items with alternatively direct and inverted items. SUS uses a 5-point Likert scale

(1 = “strongly disagree”; 5 = “strongly agree”). This scale has been validated, and is widely used. The items were scored in two different ways regarding whether these questions were direct or inverted:

- Direct items: $score = response - 1$
- Inverted items: $score = 5 - response$

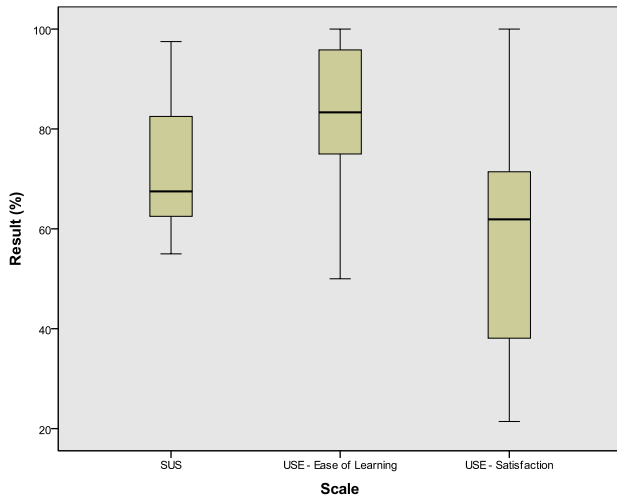


FIGURE 11. Boxplot of the questionnaire results from the user study.

The sum of the scores of all the items was in the 0 - 40 range for each replied questionnaire. In order to obtain a score in the 0 - 100, the original score was multiplied by 2.5.

The other scale was Usefulness, Satisfaction, and Ease of use questionnaire (USE) [25]. This scale has four independently validated dimensions, and we only used the dimensions of (a) ease of learning and (b) satisfaction. All the items were directly related with the corresponding feature, without using inverted questions. The questions were answered with a 7-point Likert scale. Each item was assessed with a value in the 0 - 6 range. Each dimension was converted to a 0-100 range by multiplying the sum of all the responses by $100/\maxScore$ where \maxScore was the maximum summed score in the corresponding dimension.

4) RESULTS

All the participants successfully completed all the tasks. It is worth mentioning that in the rearrangement task of the the third test, the participants faced to something new, because they had never learned how to reorder items in the priority list. The participants used two ways to address this task. The first way was to drag and drop elements from one position to another of the same list. The other way was to remove elements by dragging them outside the priority list and then to add them again in the priority list in the corresponding order. Regardless of the methods used by participants, all of them were able to successfully finish this task of the third test.

Figure 11 presents the results of the validated scales with a boxplot. The highest-ranked feature of the app was the ease of learning dimension from the USE scale, with a mean value of 82.94%. Thus, PriorityNet app was easy to learn according to the validated scale. This is also confirmed by the fact that all users figured out how to alter an existing priority list.

The second ranked feature was the usability measured with the SUS scale with an average value 72.26%. This reflects the high usability of the app, showing that the user interface of the app was probably properly designed. The last

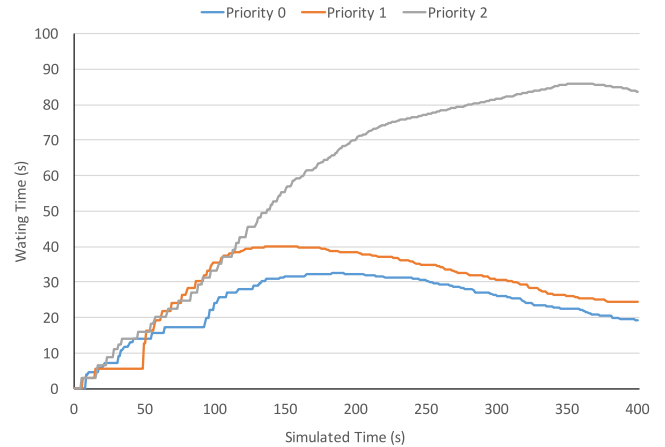


FIGURE 12. Waiting times for 35 services/second without penalizing selfish agents.

feature obtained a 57.48% average value in the satisfaction dimension from the USE scale. This dimension was probably the least ranked since participants did not observe the whole utility of the app in the short tasks of the user study. For example, they did not experience the fast communications and services for real important matters in their lives after configuring their priority preferences.

We conducted paired t-tests [26] for assessing the significances of the differences in all the possible pairs among the analyzed usability dimensions 2. One can observe that ease of learning had significant differences from the other two dimensions with a significance level of 0.001. The difference between usability and satisfaction was also significant, but with a higher significance level of 0.002.

D. COMPARISON OF WAITING TIMES FOR SERVICES CONSIDERING PRIORITIES

In order to further assess the current approach, we performed simulations with the ABS-SmartPriority application. We executed 100 agents simulating users that requested services with different priorities. These agents took nondeterministic decisions based on their goals following TABSAOND (a technique for developing agent-based simulation apps and online tools with nondeterministic decisions) [27]. The simulator simulated a duration of 400 s in each execution. Figure 12 shows an example in a smart city that was able to deliver 35 services per second for these 100 agents. This simulation did not penalize selfish users that overused high priorities. One can observe that the system was able to properly attend high-priority requests faster.

In addition, we executed a simulation in which the smart city was only able to attend 15 services per second, without using the penalization mechanism. Figure 13 shows the results. In this case, the overload of requests made the system not to be able to attend urgent requests faster.

Furthermore, the current approach was simulated with a priority mechanism in which some users could be penalized by lowering the priorities of the requests in case they had

TABLE 2. Paired t-test results for comparing the results about the different features of the app.

		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference		t	df	Sig. (2-tailed)
					Lower	Upper			
Pair 1	SUS - USE Ease of Learning	-10.67429	12.97284	2.83091	-16.57945	-4.76912	-3.771	20	.001
Pair 2	SUS - USE Satisfaction	14.77810	18.51249	4.03976	6.35131	23.20488	3.658	20	.002
Pair 3	USE Ease of Learning - USE Satisfaction	25.45238	25.2834	5.50964	13.95948	36.94529	4.620	20	.000

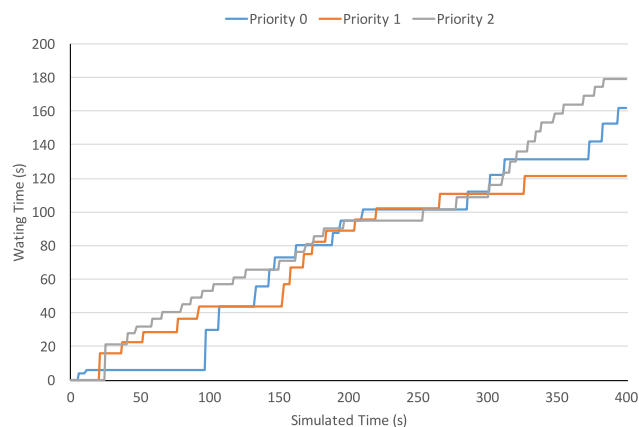


FIGURE 13. Waiting times for 15 services/second without penalizing selfish agents.

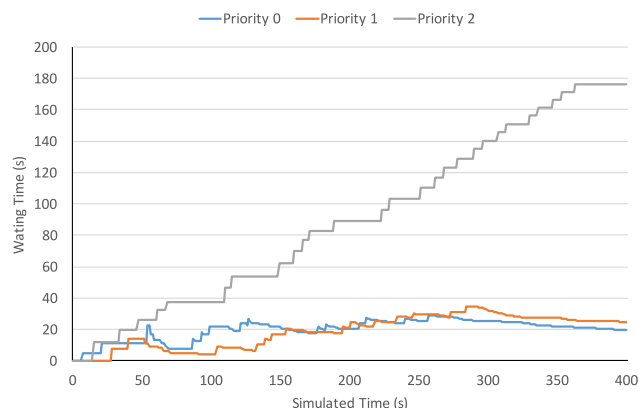


FIGURE 14. Waiting times for 15 services/second penalizing selfish agents.

overused high-priority requests. The rate of attended services was the same as in the previous case. Figure 14 presents the results. This penalization mechanism allowed the system to attend faster the high-priority requests.

V. CONCLUSIONS AND FUTURE WORK

This work has presented a novel app that allows users to dynamically establish priorities. This is useful for prioritizing different services and fastening urgent services in smart cities with ultra-dense networks. This opens a new channel of communication between smart cities and citizens. The app has

showed a high level of usability, especially in ease of learning. This app has also shown its proper scalability when increasing the list priority size in terms of response time for uploading preferences. Some agent-based simulations showed that the proposed approach allows attending urgent services faster.

The current work is planned to be extended by allowing users to activate an automatic mode. In this mode, the app would automatically select the prioritized list of services based on the particular history of the corresponding user. For instance, if the user normally establishes a service as urgent in the weekdays and removes it from the list in weekends, the app would follow a similar pattern in automatic mode.

REFERENCES

- [1] C. Galiotto, N. K. Pratas, L. Doyle, and N. Marchetti, "Effect of LOS/NLOS propagation on 5G ultra-dense networks," *Comput. Netw.*, vol. 120, pp. 126–140, Jun. 2017.
- [2] P. Lynggaard and K. E. Skouby, "Deploying 5G-technologies in smart city and smart home wireless sensor networks with interferences," *Wireless Pers. Commun.*, vol. 81, no. 4, pp. 1399–1413, Apr. 2015. [Online]. Available: <https://doi.org/10.1007/s11277-015-2480-5>
- [3] Z. Zhang, C.-H. Lung, I. Lambadaris, and M. St-Hilaire, "When 5G meets ICN: An ICN-based caching approach for mobile video in 5G networks," *Comput. Commun.*, vol. 118, pp. 81–92, Mar. 2017.
- [4] M. Taha, L. Garcia, J. M. Jimenez, and J. Lloret, "SDN-based throughput allocation in wireless networks for heterogeneous adaptive video streaming applications," in *Proc. 13th Int. IEEE Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 963–968.
- [5] M. Taha, L. Parra, L. Garcia, and J. Lloret, "An Intelligent handover process algorithm in 5G networks: The use case of mobile cameras for environmental surveillance," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2017, pp. 840–844.
- [6] J. Lloret, L. Parra, M. Taha, and J. Tomás, "An architecture and protocol for smart continuous eHealth monitoring using 5G," *Comput. Netw.*, vol. 129, pp. 340–351, Dec. 2017.
- [7] B. Blanco et al., "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN," *Comput. Standards Interfaces*, vol. 54, pp. 216–228, Nov. 2017.
- [8] T. Anagnostopoulos, K. Kolomvatos, C. Anagnostopoulos, A. Zaslavsky, and S. Hadjiefthymiades, "Assessing dynamic models for high priority waste collection in smart cities," *J. Syst. Softw.*, vol. 110, pp. 178–192, Dec. 2015.
- [9] I. García-Magariño and R. Lacuesta, "ABS-SmartPriority: An agent-based simulator of strategies for managing self-reported priorities in smart cities," *Wireless Commun. Mobile Comput.*, vol. 2017, 2017, Art. no. 7254181. [Online]. Available: <https://doi.org/10.1155/2017/7254181>
- [10] K. E. Skouby and P. Lynggaard, "Smart home and smart city solutions enabled by 5G, IoT, AAI and CoT services," in *Proc. Int. Conf. IEEE Contemp. Comput. Informat. (IC3I)*, Nov. 2014, pp. 874–878.

- [11] I. Chatzigiannakis, "Apps for smart buildings: A case study on building security," in *Start-Up Creation: The Smart Eco-Efficient Built Environment*. Sawston, U.K.: Elsevier, 2016, pp. 465–479.
- [12] P. Gora and I. Rüb, "Traffic models for self-driving connected cars," *Transp. Res. Procedia*, vol. 14, pp. 2207–2216, Apr. 2016.
- [13] A. S. Rao and M. P. Georgeff, "Modeling rational agents within a BDI-architecture," in *Proc. KR*, 1991, pp. 473–484.
- [14] I. Ucar, C. Donato, P. Serrano, A. Garcia-Saavedra, A. Azcorra, and A. Banchs, "On the energy efficiency of rate and transmission power control in 802.11," *Comput. Commun.*, vol. 117, pp. 164–174, Feb. 2018. [Online]. Available: <https://doi.org/10.1016/j.comcom.2017.07.002>
- [15] K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, and W. Xiang, "Big data-driven optimization for mobile networks toward 5G," *IEEE Netw.*, vol. 30, no. 1, pp. 44–51, Jan./Feb. 2016.
- [16] B.-J. Chang and S.-H. Liou, "Adaptive cooperative communication for maximizing reliability and reward in ultra-dense small cells LTE-A toward 5G cellular networking," *Comput. Netw.*, vol. 115, pp. 16–28, Mar. 2017.
- [17] J. Seyedmohammadi, F. Sarmadian, A. A. Jafarzadeh, M. A. Ghorbani, and F. Shahbazi, "Application of SAW, TOPSIS and fuzzy TOPSIS models in cultivation priority planning for maize, rapeseed and soybean crops," *Geoderma*, vol. 310, pp. 178–190, Jan. 2018.
- [18] R. Sudarsan and C. J. Ribbens, "Combining performance and priority for scheduling resizable parallel applications," *J. Parallel Distrib. Comput.*, vol. 87, pp. 55–66, Jan. 2016.
- [19] S. Binder, Y. Maknoon, and M. Bierlaire, "Exogenous priority rules for the capacitated passenger assignment problem," *Transp. Res. B, Methodol.*, vol. 105, pp. 19–42, Nov. 2017.
- [20] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "PASCOC: Priority-based application-specific congestion control clustering protocol," *Comput. Netw.*, vol. 74, pp. 92–102, Dec. 2014.
- [21] E.-J. Kim, M. Kim, S.-K. Youm, S. Choi, and C.-H. Kang, "Priority-based service differentiation scheme for IEEE 802.15.4 sensor networks," *AEU-Int. J. Electron. Commun.*, vol. 61, no. 2, pp. 69–81, 2007.
- [22] C. Bernardoff, *NGUI for Unity*. Birmingham, U.K.: Packt, 2014.
- [23] I. García-Magariño, R. Lacuesta, and J. Lloret, "ABS-FishCount: An agent-based simulator of underwater sensors for measuring the amount of fish," *Sensors*, vol. 17, no. 11, p. 2606, 2017.
- [24] J. Brooke et al., "SUS—A quick and dirty usability scale," *Usability Eval. Ind.*, vol. 189, no. 194, pp. 4–7, 1996.
- [25] A. M. Lund, "Measuring usability with the use questionnaire¹²," *Usability Interface*, vol. 8, no. 2, pp. 3–6, 2001.
- [26] H. Hsu and P. A. Lachenbruch, "Paired *t* test," in *Wiley Encyclopedia of Clinical Trials*. Hoboken, NJ, USA: Wiley, 2008.
- [27] I. García-Magariño, G. Palacios-Navarro, and R. Lacuesta, "TABSAOND: A technique for developing agent-based simulation apps and online tools with nondeterministic decisions," *Simul. Model. Pract. Theory*, vol. 77, pp. 84–107, Sep. 2017.



FRANKS GONZÁLEZ-LANDERÓ received the degree in computer science engineering from the University of Zaragoza in 2012, where he is currently pursuing the Ph.D. degree. He did his master's thesis in computer graphics, videogames, and virtual reality at the University Rey Juan Carlos of Madrid in 2016. He adapted his engineering grade to the European University Education System in 2017. He has been a Computer Science Engineer with Edison Desarrollos since 2015. He has specialized in mobile application development with several courses, with topics, such as Android and Corona SDK. He has professional experience in mobile application development with a cross-platform engine and devices, such as Microsoft Kinect. His research interests include mobile application development, usability, and agent-based simulators.



IVÁN GARCÍA-MAGARIÑO received the Ph.D. degree in computer science engineering from the Complutense University of Madrid in 2009. He was a Lecturer with Madrid Open University from 2010 to 2014. He has been a Lecturer with the University of Zaragoza since 2014. He belongs to the EduQTech research group. Among journals, book chapters, conferences, and workshops, he has over 100 publications (36 in journals with ISI Thomson JCR). His most relevant publications belong to international journals with a high impact, such as *Engineering Applications of Artificial Intelligence*, *Expert Systems With Applications*, *Information Sciences*, *Knowledge-Based Systems*, *Information and Software Technology*, *Simulation Modelling Practice and Theory*, *Journal of Systems and Software*, *Personal and Ubiquitous Computing*, *International Journal of Medical Informatics*, *Medical and Biological Engineering and Computing*, *Journal of Biomedical Informatics*, and *Computer Standards and Interfaces*. He was a recipient of the FPI Researcher Scholarship from 2006 to 2010.



RAQUEL LACUESTA (M'17) received the degree in computer science engineering and the Ph.D. degree (Dr.Eng.) in computer science engineering from the Polytechnic University of Valencia, in 1999 and 2008, respectively. She has been a Lecturer of Computer Science with the University of Zaragoza, for over 12 years, where she currently teaches human-computer interaction, security, and databases subjects. She has authored or co-authored over 30 scientific papers published in national and international conferences, over 15 papers about education published in national and international conferences, and several papers published in international journals. Her main topics of research are security and auto-configuration on ad hoc and spontaneous networks, the design and evaluation of routing algorithms, computer-human interaction, and education. She has been involved as an Organizer and Chair for several important program committees of international conferences. She is an Associate Editor and Reviewer of the *International Journal Networks Protocols and Algorithms* and a member of different national research projects.



JAIME LLORET (M'07–SM'10) received the M.Sc. degree in physics in 1997, the M.Sc. degree in electronic engineering in 2003, and the Ph.D. degree in telecommunication engineering (Dr.Eng.) in 2006. He is currently an Associate Professor with the Universitat Politècnica de Valencia. He is the Chair of the Integrated Management Coastal Research Institute and the Head of the Active and Collaborative Techniques and Use of Technologic Resources in the Education Innovation Group. He is the Director of the University Diploma Redes y Comunicaciones de Ordenadores and the University Master Digital Post Production. He leads many national and international projects. He has authored 22 book chapters and over 360 research papers published in national and international conferences and international journals (over 140 with ISI Thomson JCR). He is an IARIA Fellow. He has been the Internet Technical Committee Chair (the IEEE Communications Society and the Internet Society) from 2013 to 2015. He is the IARIA Journals Board Chair for eight journals. He is currently the Chair of the Working Group of the Standard IEEE 1907.1. He has been a general chair (or co-chair) of 39 international workshops and conferences. He has been involved in over 320 program committees of international conferences, and over 130 organization and steering committees. He has been a co-editor of 40 conference proceedings and a guest editor of several international books and journals. He is the Editor-in-Chief of *Ad Hoc and Sensor Wireless Networks* (with ISI Thomson Impact Factor), the *International Journal of Networks Protocols and Algorithms*, and the *International Journal of Multimedia Communications*. He has been an associate editor of 46 international journals (16 with ISI Thomson Impact Factor).

• • •

6.4. Green communication for tracking heart rate with smartbands.

Cita completa:

GONZÁLEZ-LANDERO, F., GARCÍA-MAGARIÑO, I., LACUESTA, R., & LLORET, J. (2018). Green communication for tracking heart rate with smartbands *Sensors*, 18(8), 2652.

Abstract:

The trend of using wearables for healthcare is steeply increasing nowadays, and, consequently, in the market, there are several gadgets that measure several body features. In addition, the mixed use between smartphones and wearables has motivated research like the current one. The main goal of this work is to reduce the amount of times that a certain smartband (SB) measures the heart rate (HR) in order to save energy in communications without significantly reducing the utility of the application. This work has used an SB Sony 2 for measuring heart rate, Fit API for storing data and Android for managing data. The current approach has been assessed with data from HR sensors collected for more than three months. Once all HR measures were collected, then the current approach detected hourly ranges whose heart rate were higher than normal. The hourly ranges allowed for estimating the time periods of weeks that the user could be at potential risk for measuring frequently in these (60 times per hour) ranges. Out of these ranges, the measurement frequency was lower (six times per hour). If SB measures an unusual heart rate, the app warns the user so they are aware of the risk and can act accordingly. We analyzed two cases and we concluded that energy consumption was reduced 83.57% in communications when using training of several weeks. In addition, a prediction per day was made using data of 20 users. On average, tests obtained 63.04% of accuracy in this experimentation using the training over the data of one day for each user.

Article

Green Communication for Tracking Heart Rate with Smartbands

Franks González-Landero ¹ , Iván García-Magariño ^{2,3,*} , Raquel Lacuesta ^{2,3}  and Jaime Lloret ⁴ 

¹ Edison Desarrollos, 44002 Teruel, Spain; gonzalezfranks@edisondesarrollos.es

² Department of Computer Science and Engineering of Systems, University of Zaragoza, 44003 Teruel, Spain; lacuesta@unizar.es

³ Instituto de Investigación Sanitaria Aragón, University of Zaragoza, 50009 Zaragoza, Spain

⁴ Integrated Management Coastal Research Institute, Universitat Politècnica de València, 46022 València, Spain; jlloret@dcom.upv.es

* Correspondence: ivangmg@unizar.es; Tel.: +34-978-645-348

Received: 1 July 2018; Accepted: 10 August 2018; Published: 13 August 2018



Abstract: The trend of using wearables for healthcare is steeply increasing nowadays, and, consequently, in the market, there are several gadgets that measure several body features. In addition, the mixed use between smartphones and wearables has motivated research like the current one. The main goal of this work is to reduce the amount of times that a certain smartband (SB) measures the heart rate (HR) in order to save energy in communications without significantly reducing the utility of the application. This work has used an SB Sony 2 for measuring heart rate, Fit API for storing data and Android for managing data. The current approach has been assessed with data from HR sensors collected for more than three months. Once all HR measures were collected, then the current approach detected hourly ranges whose heart rate were higher than normal. The hourly ranges allowed for estimating the time periods of weeks that the user could be at potential risk for measuring frequently in these (60 times per hour) ranges. Out of these ranges, the measurement frequency was lower (six times per hour). If SB measures an unusual heart rate, the app warns the user so they are aware of the risk and can act accordingly. We analyzed two cases and we conclude that energy consumption was reduced in 83.57% in communications when using training of several weeks. In addition, a prediction per day was made using data of 20 users. On average, tests obtained 63.04% of accuracy in this experimentation using the training over the data of one day for each user.

Keywords: body sensor networks; eHealthcare; wearable sensors; heart rate; Google fit; smartband

1. Introduction

Heart diseases such as myocardial infarction or tachycardia have taken lot of human lives over the years [1]. In most cases, these unfortunate situations are treatable or even avoidable. A huge percentage of the world population does not live an appropriate lifestyle, and some conditions may provoke heart disease. Excess of alcohol, fat, tobacco, stress and lack of physical activity contribute to increasing the risk of suffering an infarct [2]. Luckily, over time, people have become more aware about these risks, and taken the appropriate actions to avoid these problems. With respect to science and technology, this is an event that does not go unnoticed either. In fact, thanks to medical science, it is known that a routine of physical activity reduces probability of suffering heart attacks, and, due to this fact, it is normal to see campaigns against obesity and junk food. Regarding technology, the world population has at their disposal hundreds of instruments and tools that promote physical activity and a healthy lifestyle. Some of these tools could be smartbands (SBs), straps, smart sneakers or any device not

intrusive that a user can wear. These devices called wearables, apart from promoting the movement, also measure several features of human body such as the footsteps of each day, blood pressure, breathing rate, heart rate, electrical activity of the heart, oxygen saturation in the blood, heart rate variability, and so on [3]. Measuring such features on children allow their caregivers to monitor them at every moment [4]. Chronic patients can improve their quality of life and reduce economic costs by means of an architecture for continuous e-Health monitoring with wearable devices and 5G, in which this service can be provided to a large amount of patients [5]. In addition, the measurement of heart rate variability with a smartband for determining stress level can improve wellbeing of people by guiding them in selecting the appropriate neighborhoods for living in [6]. Depending on preferences and needs of users, many of them prefer to wear the most comfortable and smallest wireless device. They would usually choose a device that ideally does not produce dependencies; in other words, a device that does not need to be cleaned frequently, barely needs to be charged electrically and is difficult to be damaged.

In this context, the current proposal promotes the low frequency of charging. In particular, this article proposes an approach for saving energy when safely warning a user about its heart rate activity. The way of saving energy consists of predicting the hourly ranges in which the users have a high heart rate. Then, the SB only will measure certain moments with normal frequency and at other moments with low frequency. Normal frequency means that SB will measure every minute during some established period of times and low frequency means that SB will measure each 10 min during a period of time without any risk for the user. With less measure, the SB will measure a lower number of times, and consequently it will save energy consumption. Estimating the heart rate allows for notifying to a certain user when their pulsations are out of normal range—in other words, when they may suffer a problem involved with their heart. In situations like myocardial infarction, tachycardia or Epilepsy [7], one of the common symptoms is a high heart rate in resting state, and acting on time may mean saving a life. Although heart rate is not the only factor to cover all heart diseases, it may be a strong predictor of cardiovascular death in elderly men [8] and people with other types of features [9]. Prolonging the autonomy time of an SB through the energy saving on measurements causes user dependencies on a wearable to decrease. In addition, the efficient use of energy allows the devices to satisfy user demands. The information technologies (IT) play a fundamental role with an increasing relevance on society. If we compare the current situation with 20 years ago, one can find a lot of devices and computers in homes and companies. Thus, the impact on the environment each time is more negative probably because of the generation and usage of IT equipment. The green computing does not mean bringing back the epoch before digital revolution. It means being aware of the usage of energy and devices that surround us. We are conscious about the benefits and opportunities that IT offers, thus we bet for green computing through this paper because the IT by itself provides smart solutions in order to reduce energy at home and production of goods and services. This reduction contributes directly to reducing contaminant emissions of CO_2 and, in this way, the current approach fulfills the green computing goals.

The current work is organized as follows. The next section analyzes the related work highlighting the gaps of the literature covered by the current approach. Section 3 describes the current green computing approach for tracking and warning the users about heart rate activity. Section 4 describes the experiments for validating the current approach, and Section 5 indicates and discusses the main results. Section 6 mentions the conclusions and depicts some future research lines.

2. Related Work

The research community is actively involved in the topic being treated here; for instance, one can find projects like [10] about testing security threats on a commercial smartband. In particular, their study used an illegal device pairing attack, the fake wearable gateway attack and the insecure code based attack. They observed that these attacks were able to actually intrude healthcare applications about wearable sensors. Pretz et al. [11] presented an efficient and low-cost communication architecture for

connecting smartbands. Their approach allowed one to perform N:M communications between several smartbands and several devices. In their approach, they used several concentrators. Their purpose was the continuous postoperative care of patients. Lee et al. [12] proposed a continuous Electrocardiogram (ECG) monitoring with the principles of green computing. In particular, they used the low-consuming Raspberry Pi board for managing and storing the information. This information was available on a website in which the access was only granted for the corresponding authorized personnel. Their approach had a low consumption. Iancu-Constantin et al. [13] proposed an e-health approach for remote cardiac rehabilitation using several devices for measuring different features of body. It was aimed at creating a way of communicating between a patient with heart disease and clinic personal in order to ease the monitoring of patients. It collected features such a heart rate, oxygen saturation, blood pressure and so on through an Android application. The approach achieved reducing economic costs and improved patients' quality of life, but it did not consider saving energy in communications.

In addition, Nandkishor et al. [14] exposed a very similar project to the one presented here. The purpose was to monitor different physiological parameters of patients with heart diseases. The monitoring was carried out through Body Area Network (BAN), and an Android smartphone. Finally, if a parameter was out of a certain security range, the smartphone sent an alert, through a text message or or an email, to the appropriate caregiver. The sensor that took information about physiological parameters communicated with a smartphone through Bluetooth. The smartphone stores information in a local server within a database. However, this approach did not keep energy consumption in mind. In addition, they did not explicitly mention where the information was stored. Due to this, it may be possible that their storage was not underpinned by a grand brand such as Google (Mountain View, CA, USA) and it may present some compatibility and security problems.

Moreover, Hofer et al. [15] presented another complementary project. In general terms, they proposed an interoperable personal health system. Basically, this system allowed monitoring patients with chronic obstructive pulmonary disease. The system measured several features like heartbeats, skin temperature and so on through a multi-sensor mechanism. The information was collected by a mobile device with Android and then it was stored in a server. A feature to highlight is that this approach took security into consideration because users' data were kept safe with strong security measures. Nevertheless, this paper did not consider saving energy consumption at any moment.

Furthermore, Rao et al. [16] showed e-SURAKSHAK, which was a novel cyber-physical healthcare system with service oriented architecture. The authors developed their own monitoring system that allowed measuring body temperature, heart rate, oxygen saturation level, and noninvasive blood pressure measurement. They made each system component including from sensors to power management. Their approach used end-to-end Internet connectivity provided by 6LoWPAN-based wireless network that used the 802.15.4 radio and it was verified by qualified doctors. However, it had several things lacking: (a) the system did not have any mechanism of storing information, proving measurements in real time; (b) the battery supply power was approximately only 28 h; and (c) the prototype was probably not very comfortable for being used by a patient, since their size was 120 mm × 90 mm × 55 mm.

3. Green Communications in Smart Bands for Tracking Patients with Heart Diseases

Figure 1 shows the overview of the current approach. Basically, the project is composed of six key elements, which are the activities made by a test subject, an SB, Google Fit (GF) Application Programming Interface (API), the cloud, an app for consulting certain data, and data analysis. Most of these of elements aim at giving access to user data. Due to the fact that we do not have direct access to smart band data and neither do we have access to an official API of Sony, data are extracted in a different way. When an SB is measuring, data are sent to the Google cloud. In order to access data, Google API must be used, and, to manage it, an Android app must be implemented. Subsections of this section will describe respectively most of these elements.

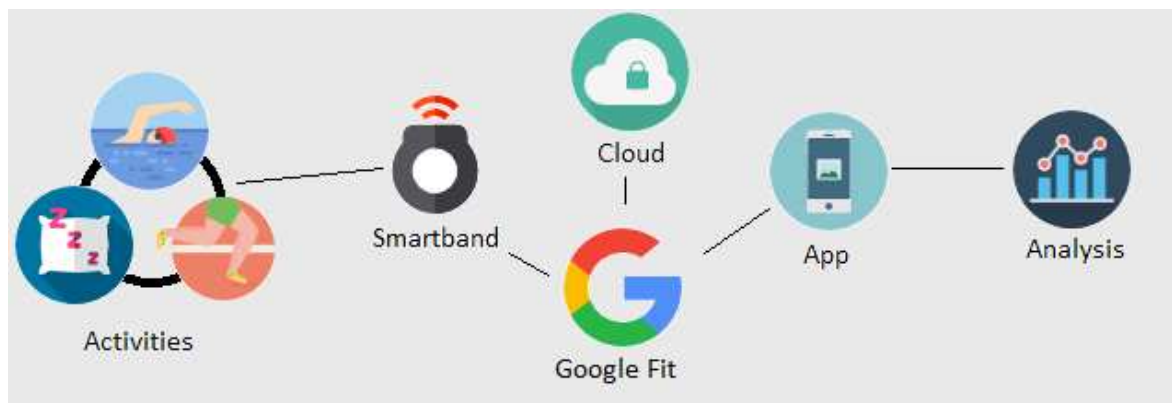


Figure 1. Overall experiment.

Figure 2 depicted the flow diagram of the algorithm in order to save energy. More concretely, it allows the reader to know how the predictions are calculated, so this way the SB will know when it must measure with more frequency. It describes the training mechanism each week. The description of Figure 2 follows. In the first step, the application compares, by each day, the average heart rate by hour with a certain threshold (t). This threshold is calculated in Equation (1). If a measurement is greater than the threshold, then we get a range with high risk. The next step consists of calculating threshold training. It is a certain threshold that allows determining if a range has high risk and consequently be measured with high frequency. Threshold training is equal to product between a certain ratio defined by us (for this particular case it is 0.8) and the average value of maximum values of heart rate for each week. The last step compares threshold training with heart rates in high risk ranges. If the comparison is positive, we add the hours belonging to high risk range as prediction. The remainder of the diagram depicts a cycling process that performs a comparison between remaining ranges, and determines if the hour exists in our prediction in order to add it or not. The prediction is obtained, first for each week and then as overlapping of all predictions by weeks. In summary, the algorithm calculates the hour intervals of three training weeks, and estimates the prediction as the overlapping of all these intervals. In the next week, it measures at high frequency the intervals estimated as risky, and with low frequency the other intervals.

Our approach works if users have a regular routine, but everyone knows, in an empirical way, that this is not always like that. Although a test subject is very disciplined and persistent with their routine, he could have a problem in order to continue it or simply, he could change their days of physical activity. Regardless of the reasons, if a test subject routine changes, risk hours could change too. In order to make the current approach adaptive to the changes of routines, we propose that the training continues with an slot of three weeks. In this way, the prediction of each week is estimated from the three previous weeks. In real life, probabilities that a certain user changes their routine is high and this is something that we must consider because otherwise the current approach would not be properly monitoring the user. We propose an algorithm in order to recalculate user's routines. The flow diagram in order to recalculate routines is depicted in Figure 3. This is a proposal to face this problem, and it will be further experimented in the future.

In the current approach, the SB is always measuring user's heart rate, at least every each 10 min, so the approach has enough data in order to know if the user's routine is changing. In order to notice the change, it will analyze data from the last three weeks. The analysis is the same that was used in order to get hour ranges with risk for user. Once the ranges have been calculated, it determines if these ranges exceed a certain threshold. If so, this range is added as a new prediction and it is marked with a flag. The last process is iterative and finishes when all hours have been added. Finally, it removes all unmarked hours, so that, in this way, we have an updated prediction. The recalculating process is performed every new week.

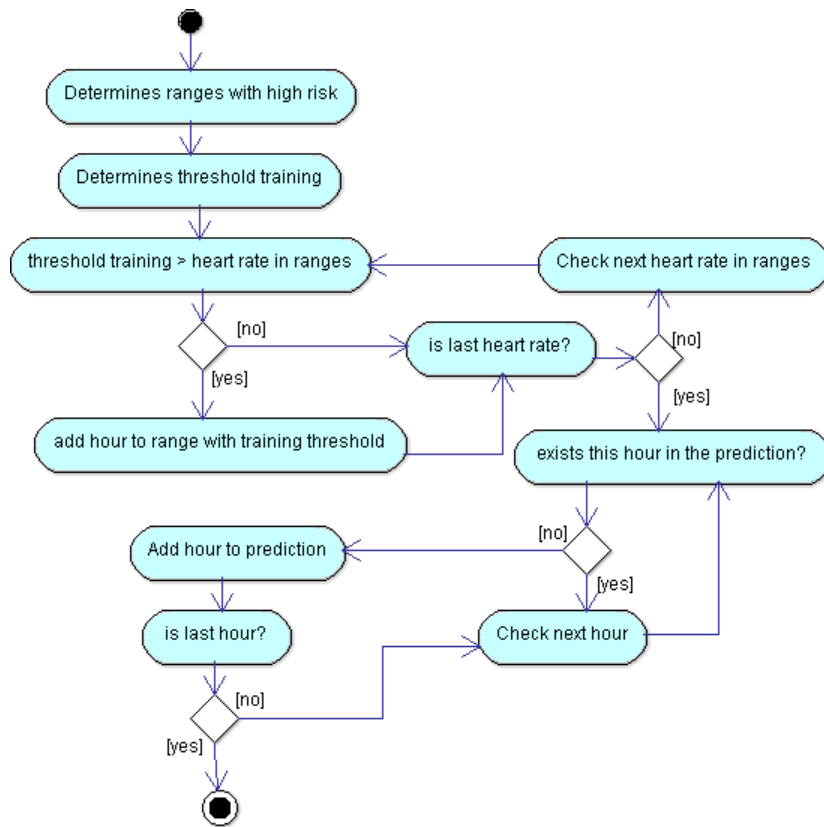


Figure 2. Algorithm for saving energy.

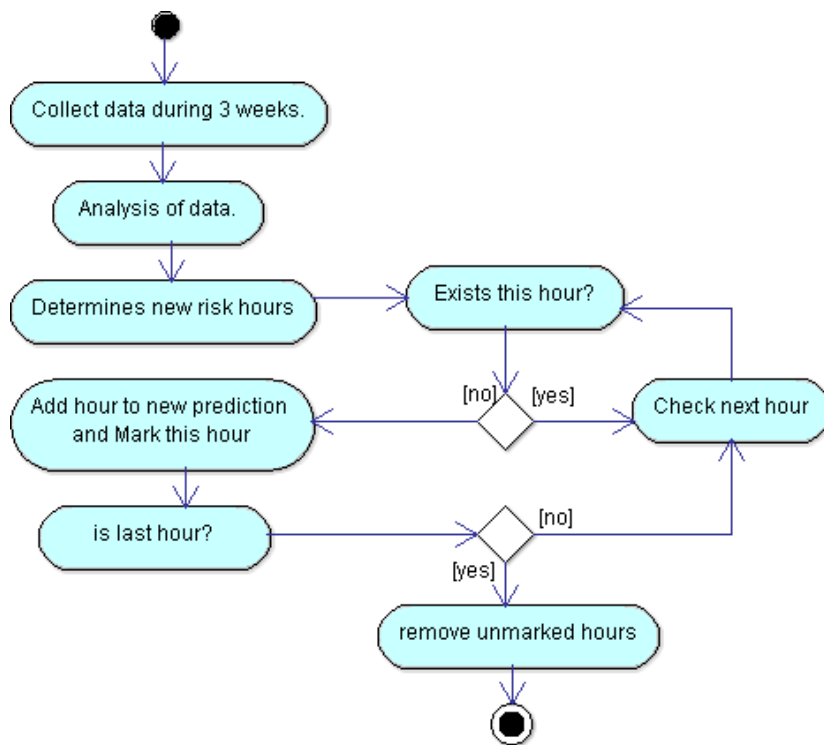


Figure 3. Diagram for recalculating user's routines.

3.1. Activities of Test Subject

The first step was to use a test subject in order to measure their heart rate in beats per minute (bpm). The only inclusion criterion was that their normal routine included physical activity. Our test person wore an SB and we measured their activity for more than three months. Our test person received instructions about SB use—for instance, he could not take off SB unless it was necessary, for example when charging the SB. The subject was informed about the experiment, and what he could do about possible risks that smart band would produce, although these were minimal. About his features, he is not a patient to any hospital, and he is not receiving any medical treatment or therapy. He is 28 years old and is male. He has declared by written consent that he gave us the permission for performing the presented experiment with him.

3.2. Smartband

In order to measure subject's heart rate, we used the Sony Smartband 2 (Minato, Tokio, Japan). This band contained a small sensor that measured heart rate and a bracelet in order to hold the sensor. The sensor measured heart rate continuously reporting measurements every minute with an ideal use. Ideal use means that the bracelet is perfectly suited to the wrist and the sensor is always clean. The sensor sends to the device's user all heart rate data; afterwards, the device sends data to the cloud through connection to the Internet. It is not necessary that the sensor is always close to the device, the sensor can store data and then, when the device is close and the Bluetooth connection is active, it sends the data to the device. We decided to use this SB for several reasons such as its affordable price and its compatibility with Google Fit (GF) API. Another reason was that this SB was waterproof. In this way, water sports could also be tracked. In particular, in our experiments, the subject practiced swimming, so the tracking of HR was also checked in water. The last reason was the amount of hours of autonomy—Sony SB 2 has autonomy up to five days in normal mode and this amount is enough, since it is possible to collect enough data. In addition, it only takes 30 min to charge the SB again.

3.3. Cloud

The main function of the Cloud is to store all data that the SB can provide. Besides the heart rate and step count collected by the SB, other information might be collected such as height and weight, and these additional data would be saved in cloud too. We cannot choose which data will be stored because this decision is managed by SB and GF API. However, we can choose which data may be downloaded, and, in this way, it is not necessary to download worthless data for our project.

3.4. The Google Fit API

Google Fit is a platform that allows developers to manage user fitness data effectively. These data may be height, weight or in our case heart rate. Developers, on behalf of users, can record, store, and read their fitness data from a repository in the Google Cloud. This management can be explained with Figure 4.

The two key components to manage fitness data properly are the Cloud and the Android Fitness APIs. In the previous section, we have already spoken about the Cloud. Android Fitness APIs are part of Google Play Services, which come as part of the Android SDK. These APIs give one access to fitness data from several different sources. The first source may be any app installed in the device, or even developed by us. Another source may be any local sensor inside the device. The remaining sources to get fitness data are from remote sources like any fitness app or sensor installed on any other device or other wearable such as SBs or straps. When a datum is read by Android Fitness API, it is always categorized in the same way. The Android Fitness API calls this categorization Data sources. Data sources represent unique sensor data. They can expose raw data coming from hardware sensors on local or companion devices. They contain data regarding the source, such as which hardware device or application generated data. Due to this, it is possible to have multiple data sources for the same

data type. For instance, one can measure heart rate from an SB in the wrist and also from a strap in chest. The Android Fitness API is composed of six sub-APIs that allow one to read, write and delete fitness data among other operations. These six sub-APIs are: Sensors API, Recording API, History API, Sessions API, Bluetooth Low Energy (BLE) API and Config API. Each one of them has a function. In this project, the most relevant APIs are History API and Sensor API. The former has allowed us to extract information to analyze data for determining whether the current approach was possible. The History API lets our application read, write and delete history data. It supports the batch import of data from the fitness history. With History API, our application can have access to any fitness data in past date and then these data can be managed and analyzed in different ways. The Sensor API makes it possible to collect real-time information for warning users when necessary.

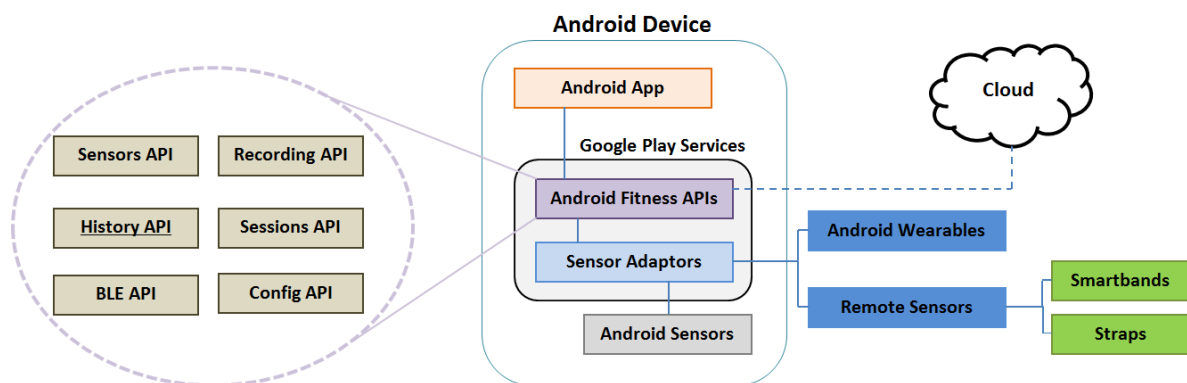


Figure 4. Google Fit.

3.5. The Android App

The main goal of the app is to know, for a certain date, which hourly ranges are classified as risky. For these classifications, the app detected the ranges in which the heart rate exceeded a certain threshold. This threshold is calculated as a weighted average between maximum value of heart rate and minimum value of heart rate belonging to certain date. The weighted average calculation is shown in the following equation:

$$t = \frac{R_{max} \cdot 2}{3} + \frac{R_{min}}{3}, \quad (1)$$

where t is the threshold, R_{max} and R_{min} are the maximum and minimum values of heart rate, respectively. A weighted average is necessary because the purpose is only to detect the cases in which the user will be at risk of a heart attack. If we had used a normal average (no weighted average), it would not have been possible to detect many important situations (we would detect all situations where the threshold would be above the average and would not necessarily represent a risk case). Analyzing only cases with high risk (using weighted average) is important in order to save energy in the measurement of heart rate and communications. This app requires user's authorization before the application can read or write any fitness sensor data. Hence, to get user authorization, it was necessary to register the application in the Google developer console. We also used Google developer console in order to indicate which Google APIs the app was going to use. The following steps summarize this process:

- Create a project in console. It is not compulsory that the project name in the console matches the project name on Integrated Development Environment (IDE) like Android Studio.
- Find and select Fitness API from the APIs and Auth console menu.
- Create a new client ID in Credential console menu. In order to create a new client ID, it is necessary to write applications details, mark the application like an Android application, write the name of application, provide the result of the SHA1 (Secure Hash Algorithm 1) for the signing certificate and indicate the application package name from of manifest file.

After finishing the registration in Google developer console, the user has to provide their permissions. When the user launches the app for the first time, a pop-up window shows the required permissions. Once the user gives their consent, the app can access the fitness data. The app architecture is depicted in Figure 5. The app was developed for Android. MainActivity is an Android Activity and shows the first screen of the application to users. The purpose of this class is to welcome users. HeartRateByDay is an instance of Android activity and represents the core of the application. It allows the app to query fitness data from a selected date using the History API.

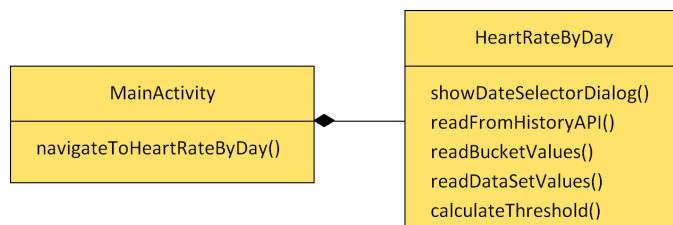


Figure 5. Diagram of class.

The most important methods of the proposed app are explained below:

- **showDateSelectorDialog():** shows a dialog window that allows the user to introduce a date in order to get the greatest heart rate to date. Finally, with a selected date, it invokes the readFromHistoryAPI() method.
- **readFromHistoryAPI():** Using the selected date and data type like a parameters, this method realizes queries in order to get the maximum value of heart rate, minimum value of heart rate and all values of heart rates for a certain date. Finally, readBucketValues() is invoked in order to manage the data. GF API has a hierarchy to order all the downloaded information. The hierarchy model is based on a layers model, in which each layer received information from another layer inside. In order to get the proper data through layers, it is necessary to follow the path depicted in Figure 6. The data are received thanks to DataReadResult class. This class contains the other classes (see Figure 6 from left to right) and it is possible to access information thanks to the methods below. These methods help us to keep legibility of code.
- **readBucketValues():** Inside DataReadResult, there is a list of objects of Bucket class. A bucket represents a time interval in which data is computed. For example, a bucket can represent a user's average speed and average heart rate over each one-hour interval. In a similar way, inside a Bucket object, there are a list of DataSet objects. A DataSet represents a fixed set of data points in a data type's stream from a particular data source. A data set usually represents data at fixed time boundaries, and can be used both for batch data insertion and as a result of read requests. Every DataSet is managed by readDataSetValues() method.
- **readDataSetValues():** This method extracts from each DataSet a DataPoint object. DataPoint represents a single data point in a data type's stream from a particular data source. A data point holds a value for each field, a timestamp and an optional start time. Lastly, each DataPoint has access to values like maximum and minimum heart rates for a given date. As the app goes through each DataPoint, it saves each average value of heart rate per hour in order to then obtain a range of hours that exceed the average heart rate. At the same time, this method arranges all data and provides tabulated data so that these can be easily analyzed afterwards.
- **calculateThreshold():** Finally, when the flow reaches this method, all of the data have already been downloaded, and consequently it is possible to calculate the threshold. Basically, this method calculates the weighted average that was explained before, then it compares each heart rate value with the threshold, and lastly it shows the information about ranges, regarding the heart rate values. For better understanding, see Figure 7.

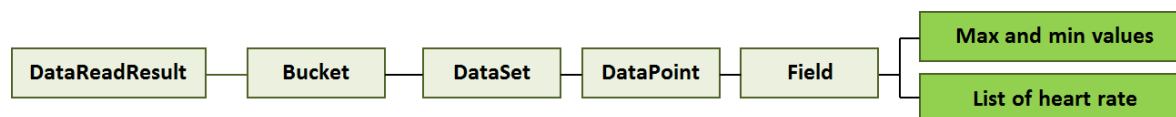


Figure 6. Hierarchy of History Application Programming Interface (API) Class.

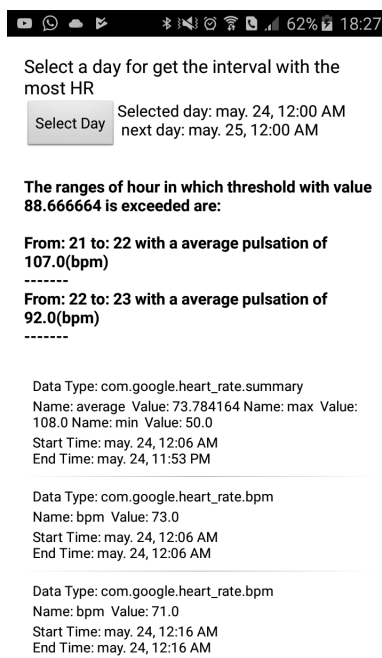


Figure 7. Screenshot of Android app.

To summarize, the HeartRateByDay method() is the one that communicates with GF API and shows all of the information about the heart rate of users for a certain day.

In Figure 6, one can observe all the application user interfaces (UIs) and at the same time how a user would see the hourly ranges where their heart rate is high. At the top of figure, a button can be seen, and its aim is to allow the user to select a date. Below this, the users can observe the value of threshold calculated for the selected day in bold font. Following this, it can be seen hour ranges with the highest values of heart rates for the selected day. From the middle of the figure to the bottom, a list with complementary information can be appreciated. The first item of list always shows the maximum value, the minimum value, and the average value of heart rate for the selected day. Remaining items show each of the values that the SB has measured in the selected day.

4. Experimentation

This section shows how collected data were analyzed. The test subject used by this project has been carrying an SB for three and a half months. The subject had two types of routines: a normal routine and a physical activity routine. In a normal routine, the test subject does not make any physical effort. Instead, he only does typical activities that any person can do such as walking, eating, studying, working in an office and so on. Physical routine refers to when the participant subject practices any sport with certain frequency.

Figure 8 depicts a graph that represents a normal routine of the participant subject. It shows all of his heart rate measurement values on Monday, 7 May 2018. It can be seen that his heart rate is practically constant between 12:00 a.m. and 8:00 a.m. because this period of time matches with his sleeping period. In this period, the heart rate maintained between 60 bpm and 70 bpm with some peaks that reached 71 or 72 bpm. The remaining measurement values belongs to a daily routine of the

test subject, which includes walking, working, studying, eating something at certain hours, and so on. The reader can notice that any remaining measure did not exceed 100 bpm. We want to highlight this point because, in the next diagram, this part is different. Finally, according to the measurement values, the maximum value of heart rate for this day was 93 bpm, and the minimum value of heart rate was 49 bpm.

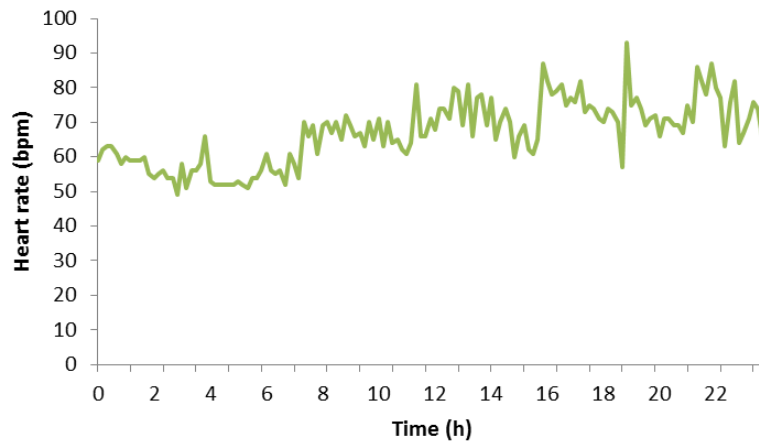


Figure 8. Heart rate in a normal day.

Figure 9 shows all the heart rates of the participant subject on Thursday, 3 May 2018. It can be seen that their heart rate was constant at the beginning of the day with values not higher than 60 bpm, very similar to the previous diagram. After 8:00 a.m., the heart rate reached values above 60 bpm, and it maintained between 60 bpm and around 80 bpm. From 9:00 p.m., the heart rate started to reach values between 100 bpm and 120 bpm since this period of time matches with physical activity period of the participant subject. During this time, he practiced swimming, and it is normal that the subject's heart rate increased. Finally, one can observe that close to the end of the graph the heart rate decreased slowly because the subject had stopped doing exercise and soon he would rest. Finally, according to measures, the maximum value of heart rate for this day was 123 bpm, and the minimum value of heart rate was 49 bpm.

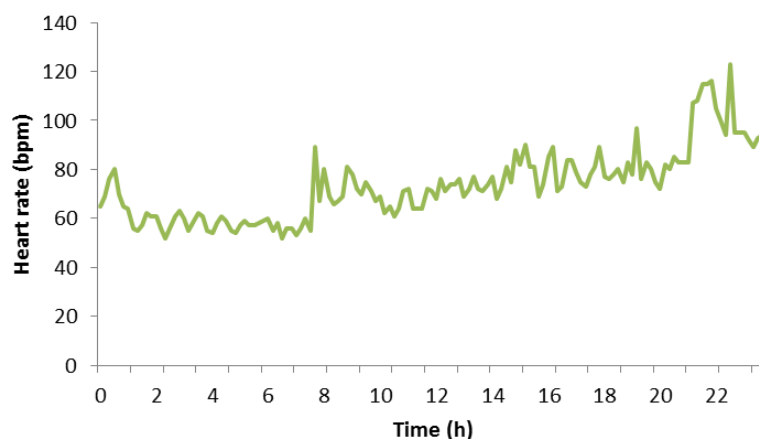


Figure 9. Heart rate in a physical activity day.

As previously mentioned, the participant subject does exercise periodically; concretely, he does exercise every Thursday. Figure 10 shows the heart rate taken on three different Thursdays. Blue represents the heart rate taken on 19 April 2018, red represents the heart rate taken on 3 May 2018 and finally green represents the heart rate taken on 10 May 2018. It can be appreciated that these

three days are very similar regarding heart rate. If we would measure another Thursday, probably we would expect another diagram very similar to these. Due to this fact, it is possible to notice a certain evolution pattern on the same days of the week but in different weeks. The pattern starts with values between 60 bpm and 80 bpm at the beginning of the day, and continues with values between 70 bpm and 100 bpm, when a participant subject is doing non-physical activities (work, study, family, etc.). In the next stage, the heart rate reached values above 100 bpm and, finally, these amounts came back to values between 80 bpm and 60 bpm. We chose these days because these were the ones with more heart rate measurements, meaning that the SB failed fewer times while trying to measure the heart rate. Hence, we needed to interpolate less data and the diagrams were more reliable. Regarding estimations, in Figure 10, we have done a linear interpolation for estimating the missing data, which represented 9.02% of the data for day one, 4.17% for day two and 3.47% for day three. Reasons why the SB did not measure well could be that their glass could be dirty, and the SB could be not properly suited to the wrist very well or the SB could have any other underwater problem. Keeping this pattern in mind, we will apply the current approach for estimating which hour ranges had the high heart rates, so these time intervals could be further monitored.

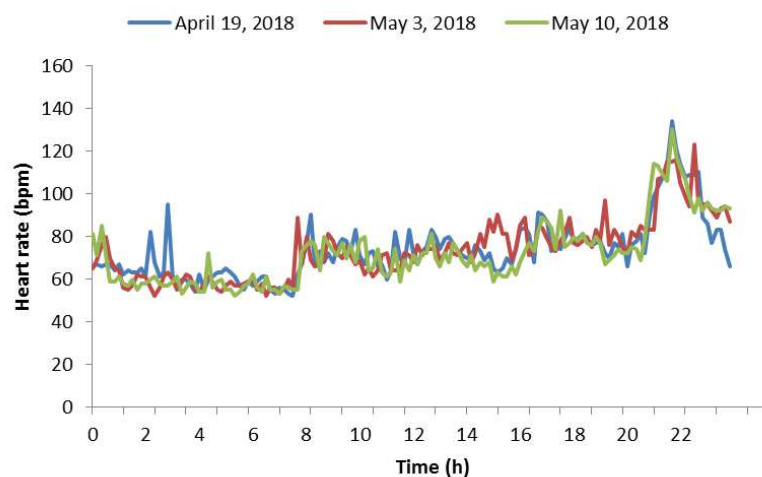


Figure 10. Heart rate of three Thursdays.

Tables 1–3 expose all the information regarding heart rate belonging to test subjects. This heart rate information was taken in three different weeks. The reader can notice that the days exposed by Figure 10 match with these three weeks. These tables contain, per column and from left to right: day of week which the heart rate was measured, maximum pulsation in current day, threshold which is calculated like weighted average of each heart rate in a day. A column called 'Range:HR' depicts risk ranges detected at each date. Each range is formed by two elements divided by colon; the first element indicates the risk hour interval and the other element depicts the value of the average heart rate for this interval. The reader must realize that this value is always greater than threshold. The remaining columns are the 'Date' that show which date that heart rate was measured and 'Range with training threshold' that includes all risk hour intervals that will belong to prediction. The first step in order to predict hour ranges is localized, which is the highest value of heart rate in every week. Then, average of maximum pulsation is calculated. In addition, a ratio threshold is established in order to calculate threshold training by multiplying the ratio threshold and the weighted average of maximum heart rate per studied week. This threshold must not be confused with the one presented in Equation (1). The result is the training threshold that indicates the limit of heart rate from which a certain heart rate is considered as high risk. To sum up, the training threshold is defined with the following equation:

$$Tt = \overline{Max(p)} \cdot Rt, \quad (2)$$

where Tt is the training threshold, $\overline{Max(p)}$ is average of maximum values of heart rate in each week and Rt is ratio threshold. Table 4 shows all the data previously described.

Once data are ordered, we establish the ranges when the SB must perform a measure. These ranges are defined by performing calculations three columns into the ‘ranges with training threshold’ column in Tables 1–3. Basically, each value in column ‘range with training threshold’ is compared. If the value belonging to any range is higher than the training threshold, this range will appear in column ‘range with training threshold’. To ease reader’s comprehension, these ranges appears in column ‘prediction’ in Table 5. These calculations represent the training of the algorithm, and the obtained ranges represent the estimations for the new week. We assess the quality of the current approach by comparing the estimated intervals with the real ones in the validation phase, in which we will refer to the corresponding week as the validation week. Thus, in this way, we can assess the accuracy of the current approach. Table 5 presents another training week with the corresponding prediction. This table is very similar to aforementioned tables. The only special attribute is the prediction column.

Table 1. Training week 1 from 16 to 22 April.

Day	Maximum Pulsation	Threshold	Ranges: Heart Rate(HR)	Date	Range with Training Threshold
Monday	121.00	99.33	-	16 April 2018	-
Tuesday	97.00	82.64	17–18:92.50 18–19:84.00 19–20:84.40	17 April 2018	-
Wednesday	108.00	89.00	-	18 April 2018	-
Thursday	134.00	106.67	21–22:118.36	19 April 2018	21–22
Friday	108.00	89.00	20–21:92.80 23–0:96.00	20 April 2018	-
Saturday	119.00	97.36	0–1:106.00 1–2:99064 2–3:110.60	21 April 2018	0–1;2–3
Sunday	117.00	97.67	16–17:102.00 17–18:107.64 20–21:100.00	22 April 2018	17–18

Table 2. Training week 2 from 30 April to 6 May.

Day	Maximum Pulsation	Threshold	Ranges:HR	Date	Range with Training Threshold
Monday	110.00	89.36	-	30 April 2018	-
Tuesday	107.00	88.67	-	01 May 2018	-
Wednesday	91.00	76.33	18–19:90 19–20:81.64 20–21:81.16 21–22:83.64 22–23:80.86	02 May 2018	-
Thursday	123.00	99.36	21–22:107.36 22–23:104.00	03 May 2018	21–22
Friday	117.00	95.36	19–20:99.25 21–22:99.64 22–23:103.60 23–0:98.00	04 May 2018	-
Saturday	114.00	95	0–1:103.50 1–2:102.36	05 May 2018	-
Sunday	98.00	84	0–1:86.50 2–3:84.20	06 May 2018	-

Table 3. Training week 3 from 7 to 13 May.

Day	Maximum Pulsation	Threshold	Ranges:HR	Date	Range with Training Threshold
Monday	93.00	78.36	16–17:78.64 21–22:79.20	07 May 2018	-
Tuesday	97.00	81.33	22–23:88.4	08 May 2018	-
Wednesday	134.00	106.00	-	09 May 2018	-
Thursday	130.00	104.00	21–22:114.40	10 May 2018	21–22
Friday	109.00	89.00	18–19:89.36 19–20:95.80 20–21:93.25 23–0:89.36	11 May 2018	-
Saturday	100.00	83.64	23–0:85.00	12 May 2018	
Sunday	87.00	75.36	0–1:83.00 1–2:77.50 14–15:78.86 15–16:76.00	13 May 2018	-

Table 4. Parameters for determining a threshold training.

Maximum Heart Rate			Average Maximum	Ratio Threshold	Threshold Training
Week 1	Week 2	Week 3			
134.00	123.00	134.00	130.33	0.80	104.27

Table 5. Validation week from 28 May to 3 June.

Day	Ranges	Date	Range with Training Threshold	Prediction
Monday	16–17:86.37 17–18:91 18–19:86.4 19–20:86.6	28 May 2018	-	-
Tuesday	16–17:89.00 17–18:94.00 18–19:89.65 19–20:89.86	29 May 2018	-	-
Wednesday	17–18:87.20 18–19:86.57	30 May 2018	-	-
Thursday	21–22:113.00	31 May 2018	21–22	21–22
Friday	16–17:85.75	01 June 2018	-	-
Saturday	11–12:86.80 23–0:91.86	02 June 2018	-	0–1 2–3
Sunday	12–13:113.50 13–14:126.36 15–16:120.5 17–18:114.36	03 June 2018	12–13 13–14 15–16 17–18	17–18

In Table 5, values inside column ‘Range with training threshold’ have been calculated the same way as in the similar previous tables. The reader can notice that hourly ranges with a high risk of suffering any heart problem for validation week are: Thursday from 21 to 22, Sunday from 12 to 14, from 15 to 16 and from 17 to 18. One can also notice that it has predicted that, on Monday, Tuesday and Wednesday, the SB must not measure because these days the subject did not have any risk. In the comparison, validation week confirms this situation—neither Monday, Tuesday or

Wednesday, the subject did not have a risk of suffering a critical situation. The next day, Thursday, it can be appreciated that the hourly range that needs special attention goes from 9:00 p.m. to 10:00 p.m. Thus, prediction column shows that the range that must be measured is exactly from 9:00 p.m. to 10:00 p.m. Thus far, this week has been perfectly predicted because the SB only has measured at the right time, but, in the following days, it will not be like that. Friday is ignored because it is the same case as Monday. On Saturday, according to the prediction, the SB must measure between 12:00 a.m. and 3:00 a.m. Nevertheless, the test subject was not at risk, and it saved energy. Last day, Sunday is the most problematic day because the prediction and ranges do not match completely. In this section, our prediction has not been completely accurate. Nevertheless, in general terms, our approach is considered appropriate. To summarize, the reader must check the accuracy of the prediction comparing 'Range with training threshold' and 'Prediction' column, if values of both columns match totally, we achieve a prediction of 100%, and conversely we achieved a different accuracy.

Now, another validation case is going to be exposed. In this case, we keep the first and second week identical and the third week goes from 4 June to 10 June, and it is presented in Table 6. In the current case, Table 7 shows the necessary parameters in order to calculate threshold training for the second validation, as in previous cases. The corresponding validation week is exposed in Table 8 and goes from 7 May to 13 May. We have decided to use this week in order to assess how similar are the results when performing the validation for two weeks.

With this second case, one can notice that the only case with risk for user belongs to Thursday from 9:00 p.m. to 10:00 p.m. The prediction made for this case considers this hour, thus user's pulsations are going to be measured more frequently in order to hold user warned about risk situations. Another topic that the current case lets us see is that the prediction is not accurate enough. If the user keeps the routine exposed on the aforementioned table, the energy would not be managed properly and it would not save energy efficiently. The solution for this inconvenience is to recalculate prediction periodically.

Table 6. Training week 4 from 4 to 10 June.

Day	Maximum Pulsation	Threshold	Ranges	Date	Range with Training Threshold
Monday	103.00	87.00	-	04 June 2018	-
Tuesday	90.00	76.64	16–17:83.40 17–18:83.50 18–19:81.50	05 June 2018	-
Wednesday	89.00	76.64	16–17:77.20 17–18:82.00	06 June 2018	-
Thursday	112.00	91.33	-	07 June 2018	-
Friday	101.00	84.36	20–21:92.25 22–23:92.50	08 June 2018	-
Saturday	104.00	86.67	14–15:92	09 June 2018	-
Sunday	94.00	80.67	16–17:85.75	10 June 2018	-

Table 7. Parameters for determining a threshold training during second validation.

Maximum Heart Rate			Average Maximum	Ratio Threshold	Threshold Training
Week 1	Week 2	Week 3			
134.00	123.00	112.00	123.00	0.80	98.40

Table 8. Validation week 2 from 7 to 13 May.

Day	Ranges	Date	Range with Training Threshold	Prediction
Monday	16–17:78.64 21–22:79.20	07 May 2018	-	-
Tuesday	22–23:88.40	08 May 2018	-	-
Wednesday	-	09 May 2018	-	-
Thursday	21–22:114.40	10 May 2018	21–22	21–22 22–23
Friday	18–19:89.36 19–20:95.80 20–21:93.25 23–0:89.36	11 May 2018	-	19–20 21–22 22–23 23–0
Saturday	23–0:85.00	12 May 2018	-	0–1 1–2 2–3
Sunday	0–1:83.00 1–2:77.50 14–15:78.86 15–16:76.00	13 May 2018	-	16–17 17–18 20–1

Before presenting the results on energy consumption, this article introduces Bluetooth’s energy expenditure because this way the energy saving can be more easily understood. Nowadays, Bluetooth 4.0 is divided into the following three types:

- *Classic Bluetooth*: The typical Bluetooth based on previous protocols.
- *Bluetooth high speed*: A type of high speed Bluetooth based on WiFi.
- *Bluetooth low energy*: Also called Bluetooth Smart, focuses on consuming little energy. This variant has been evolving with features focused on the Internet of Things.

Due to this classification, the energy that our approach spends depends on the Bluetooth technology. For example, Bluetooth classic connection is not the same as Bluetooth low energy connection. With the arrival of Internet of Things and the remaining devices connected, most devices are connected through Bluetooth low energy, if using Bluetooth. The SB used in this paper is inside this case. Keeping in mind that the energy consumption may vary between 0.01 Ws and 0.05 Ws [17], we calculated which amount is spent by Bluetooth connection in a week. Sony SB 2 can send heart rate measurements every minute; in other words, during one hour, SB has measured sixty times. Therefore, in an hour, the SB has spent 1.8 Ws on average, in 24 h, it has spent 43.2 Ws and in seven days, it has spent 302.4 Ws. The next section shows how this energy consumption can be reduced.

5. Results

In the view of the experiments followed in the proposed process, we can say that this way of saving energy seems effective, but it is not yet known how much energy is saved. Figure 11 presents the amount of energy savings from 7 May to 13 May. This graph shows energy consumption. On one hand, it shows the energy consumption without any green communication strategy (red line). On the other hand, it shows the energy consumption with our approach (blue line). In the control mechanism used for comparison, the SB performs a measure each minute, it means 60 measures per hour. On the other side, we use 0.03 Ws of average consumption with Bluetooth connection because [17] point us to the fact that consumption varies between 0.01 Ws and 0.05 Ws. If the SB measures 60 times per hour, we get that the daily consumption is 43.2 Ws, as can be seen in the diagram of Figure 11. In relation to our proposal, the SB would be measuring user heart rate each 10 minutes per hour in ranges without

risk because we cannot stop monitoring the user; nevertheless, at risk ranges, the SB must measure each minute the same way as the last case. In order to know what amount of energy is saved, we calculated energy expenditure per week with a normal use of SB, which is: $43.2 \text{ Ws} \times 7 \text{ days} = 302.4 \text{ Ws}$ of energy, we calculated energy expenditure with our approach. In order to calculate the latter, we consider the number of risk hours, which are 12, and remaining hours of the week, which are 156 h ($24 \text{ h} \times 7 \text{ days} - 12 \text{ risk hours}$) according to Table 8. Now, on this point, we calculated the energy consumption: $156 \text{ h without risk} \times 0.03 \text{ Ws} \times 6 \text{ measures per hour} = 28.08 \text{ Ws}$ and $12 \text{ h with high risk} \times 0.03 \text{ Ws} \times 60 \text{ measures per hour} = 21.6 \text{ Ws}$, The final result is $21.6 \text{ Ws} + 28.08 \text{ Ws} = 49.68 \text{ Ws}$ this week. When comparing both energy expenditures, a difference of 252.72 Ws of saving can be appreciated. In particular, the energy consumption reduction was 83.57% in this case.

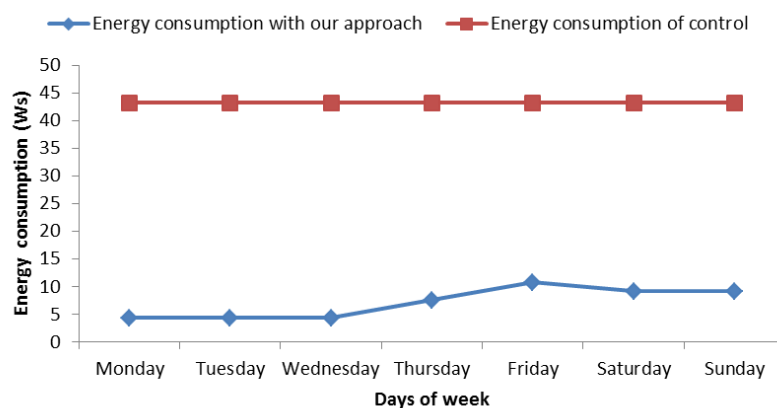


Figure 11. Energy consumption from 7 May to 13 May.

When analyzing the other case shown in Figure 12 and belonging to Table 5, it can be appreciated that the energy consumption was similar to the aforementioned one. In this case, we analyzed the week from 28 May to 3 June 2018. For this case, there were less risk hours, concretely 4 h, performing the same previous calculations, and we obtained an energy consumption reduction of 87.85%. Finally, the average energy reduction was 85.71% when considering the mean of these cases.

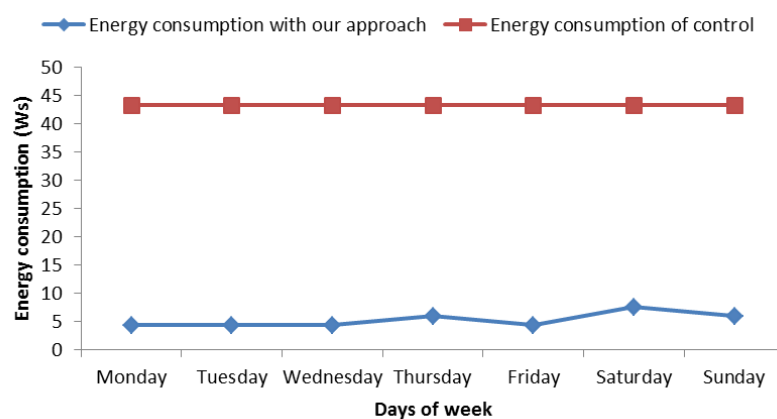


Figure 12. Energy consumption from 28 May to 3 June.

Figure 13 shows the energy consumption by a certain day, in particular 13 May 2018. The data can be consulted in Table 8. The graphic shows two types of consumptions. On the one hand, it shows the consumption of the control mechanism (red line), which represents the consumption of SB per day without any type of savings. It means that the SB measures 60 times per hour. We simulated the consumption of Bluetooth connection with random fluctuations between

0.01 Ws and 0.05 Ws inspired by the principles of simulating variations proposed in TABSAOND (a technique for developing agent-based simulation apps and online tools with nondeterministic decisions) [18], so, in this way, we can expose a more realistic consumption. The consumption has been calculated as $24 \text{ h} \times 60 \text{ measurements} \times \text{connection energy consumption}$. On the other hand, the consumption made by our proposal is represented too (blue line) and was calculated with this mentioned formula, for the risky intervals. At hours without risk, the SB measures six times per hour, thus the consumption was calculated with the formula $\text{number hours without risk} \times 6 \text{ measurements} \times \text{connection energy consumption}$. The consumption with risk hours was calculated with $\text{risk hours} \times 60 \text{ times} \times \text{connection energy consumption}$. We cannot give an exact figure of the amount of energy savings because the connection energy consumption varies between 0.01 Ws and 0.05 Ws. Nevertheless, we can provide the maximum and minimum amounts of saving energy. In the hypothetical case that the SB would measure for the whole day with 0.05 Ws and without a strategy for saving energy, we would get a maximum expenditure of $0.05 \text{ Ws} \times 60 \text{ measurements} \times 24 \text{ h} = 72 \text{ Ws}$. If we apply our approach in this case of maximum energy consumption per connection, we obtain 15.3 Ws of maximum expenditure energy. It means 78.75% of saving energy. In the case of minimum expenditure of energy per connection, we obtain 14.4 Ws without the saving-energy strategy. Applying our approach, we get 3.06 Ws, which is a 78.75% of energy consumption reduction. The energy reduction of these two cases coincides since the energy reduction does not depend on the specific value of energy consumption per connection, as long as this value is the same in all the compared cases.

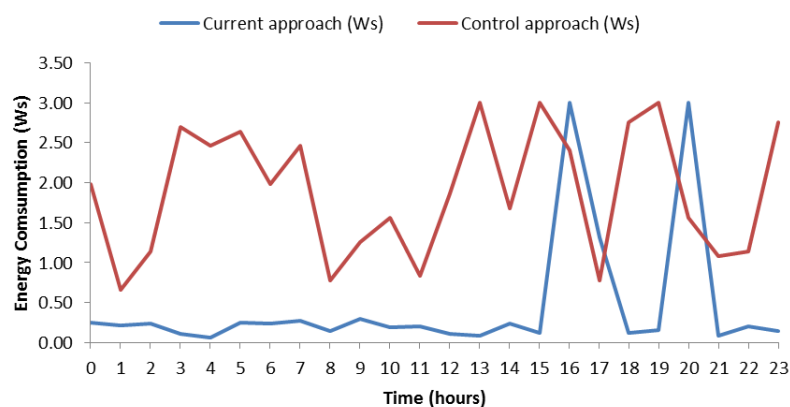


Figure 13. Energy consumption on 13 May.

In this case, the energy consumption with our approach did not reach values exceeding 0.5 Ws per hour except risk ranges where values reached up to 3 Ws approximately. In the control mechanism, the consumption fluctuated and most of the time values were higher than with our approach. In order to corroborate the savings in daily consumption, we have included Figure 14, which is similar but for the day 11 May 2018. Data can be consulted in Table 8. On this case, one can observe similar features to the ones of the aforementioned case, such as the remarkable amount of saved energy along day. Finally, it is worth highlighting that this case has one risk hour more than Figure 13, and the energy consumption was 74.99% for both minimum and maximum energy consumption per connection. Keeping both cases in mind, the average saving-energy percentage was 76.87% per day.

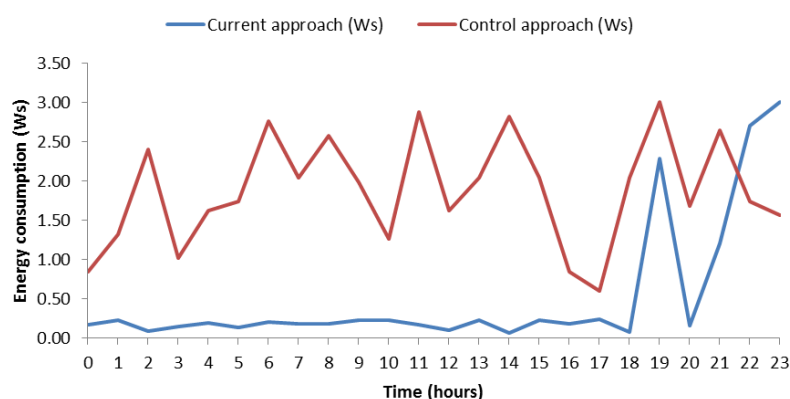


Figure 14. Energy consumption on 11 May.

In order to validate the current approach, we have further experienced it with a data set from a public repository (Physionet), which is a collection of data from users with relation in cardiac topics [19]. Due to a huge amount of files found in Physionet, we have automatized the way of extracting data to do it faster. The data about users are downloaded by means of the add-on of Google Chrome called 'Download'em all'. In this way, we downloaded all files that contain all features measured of a user, with heart rate among these. Then, with a Linux console and the 'grep' command, all heart rates have been extracted from files in order to be analyzed. To increase the reliability of our study, the approach was tested 20 times. This means with 20 users from the data set. Due to the repository only having a few days of information, the test was slightly modified. For this case, we are going to validate days instead of weeks as a consequence of the data availability with a few consecutive days from repository. Now, one day is used for establishing risk intervals in the training phase and the other day was used for validation. The way of analyzing data was similar to the aforementioned step. For each user, the first step was to establish a threshold. Then, we calculated a weighted average of maximum and minimum heart rate of the analyzed day. Due to the validation being per days instead of per weeks, we establish the maximum heart rate per hour of day, and if this heart rate was greater than threshold, the hour interval was marked as a risk hour (similarly to risky ranges). Once all hours were detected, the next step was to validate hours with the next day. At the validation phase, the hours marked like risk hours are verified if matched with risk hour on the validation day. In the affirmative case, a success was counted, and otherwise a fail was counted. In this way, accuracy percentage was calculated in relation to our approach for 20 users. Tables 9 and 10 illustrate the accuracy percentage of each user. The average accuracy of our approach was 63.04% with a standard deviation of 17.36%.

Table 9. Test with 20 users—Part I.

User	1	2	3	4	5	6	7	8	9	10
Accuracy (%)	62.50	70.83	35.29	62.50	70.00	95.00	70.00	52.63	73.68	42.10

Table 10. Test with 20 users—Part II.

User	11	12	13	14	15	16	17	18	19	20
Accuracy (%)	50.00	84.21	70.83	61.53	58.33	42.10	61.90	95.65	68.42	33.33

The individual accuracy results showed a high variability. For instance, some users obtained very high accuracies (e.g., users 6 and 18 with accuracies of 95% or above) while other users obtained low accuracies (e.g., users 3, 10, 16 and 20 with accuracies of 42% or below). It is worth highlighting the relation between obtained accuracies and the analyzed data. Both training and validation phases were

relatively short for each user, since, for each phase, we only used data from one day due to the available data of the used public repository. Thus, the whole experimentation concerning the 20 users was representative, but the individual accuracies for each user were not so representative. Thus, the nature of the used public data produced a high variability of accuracies for each user, and consequently some users had better results than others. In addition, the idiosyncrasy of each individual could have contributed to this variability. Furthermore, the data analyzed respectively by training and validation phases belonged to contiguous days. Hence, the validation phase used data from a day of the week different from the day of the week used for the training. For example, for a particular user, the training could have used data from Sunday, the validation could have been performed on Monday, and the user could have completely different routines in these two days of the week.

6. Conclusions

The current work has presented a mechanism for keeping track of the heart rate of users focusing on the time intervals of high risk with green computing. In particular, it efficiently uses the communications for reducing the energy consumption. We achieved reducing the average frequency of measurements made by an SB. This reduction did not significantly affect the SB functionality quality for this purpose, and the user will keep safe concerning heart problems that can be detected with high heart rates. More concretely, it shows that people with particular routines have periods of times where heart rate is higher than normal. Thanks to the applied green computing approach, the smart band was able to reduce the frequency of measurements by learning the routines of the user. Compared to a normal use of SB, our approach achieved 85.71% of energy consumption reduction. According to daily analysis, the maximum and minimum amount of consumption without any strategy for saving energy was 72 Ws and 14.4 Ws, respectively, and our approach achieved an average energy consumption reduction of 76.87% in these cases. In addition, in the experimentation performed with data of 20 people from a public repository, we obtained an average prediction accuracy of 63.04%.

As future work, we plan to increase the scope of the current approach to the measurement of other health indicators, such as heart rate variability or any other factor that can be measured by wearables. In this way, the time of autonomy can be increased on wearable devices. In addition, we will continue working with Google technologies because, through this paper, we have noticed that Google Fit API works with a wide range of devices. In particular, we will develop a plugin of FAMAP (a framework for developing m-Health apps) [20] for analyzing data from wearable devices with green computing, based on the findings and software of the current work. Thus, we will keep the security standards that apply to programs with Google technologies. Furthermore, we will analyze other similar projects to improve the features of this plugin, by implementing some detected missing functionalities. When we reach a high amount of health indicators, we will implement body area networks (BANs). These BANs will be interconnected with each other by means of BodyCloud [21], since it is a well-known cloud-assisted platform for m-Health applications based on wearable sensors and uses Google technologies like in the current approach.

Author Contributions: Conceptualization, Franks González-Landero, Iván García-Magariño, Raquel Lacuesta and Jaime Lloret; Methodology, Franks González-Landero, Iván García-Magariño and Raquel Lacuesta; Software, Franks González-Landero; Validation, Franks González-Landero and Iván García-Magariño; Formal Analysis, Jaime Lloret; Investigation, Franks González-Landero, Iván García-Magariño, Raquel Lacuesta and Jaime Lloret; Resources Iván García-Magariño and Raquel Lacuesta; Data Curation, Franks González-Landero and Iván García-Magariño; Writing-Original Draft Preparation, Franks González-Landero and Iván García-Magariño; Writing-Review & Editing, Raquel Lacuesta and Jaime Lloret; Visualization, Franks González-Landero, Iván García-Magariño and Jaime Lloret; Supervision, Iván García-Magariño and Raquel Lacuesta; Project Administration Iván García-Magariño and Raquel Lacuesta; Funding Acquisition, Iván García-Magariño, Raquel Lacuesta and Jaime Lloret

Funding: This work acknowledges the research project “Construcción de un framework para agilizar el desarrollo de aplicaciones móviles en el ámbito de la salud” funded by the University of Zaragoza and Foundation Ibercaja with grant reference JIUZ-2017-TEC-03. We also acknowledge support from “Universidad de Zaragoza”,

“Fundación Bancaria Ibercaja” and “Fundación CAI” in the “Programa Ibercaja-CAI de Estancias de Investigación” with reference IT1/18.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

GF	Google Fit
SB	Smartband
bpm	beats per minute
HR	Heart Rate

References

- Mendis, S.; Thygesen, K.; Kuulasmaa, K.; Giampaoli, S.; Mähönen, M.; Ngu Blackett, K.; Lisheng, L.; Writing Group on behalf of the Participating Experts of the WHO Consultation for Revision of WHO Definition of Myocardial Infarction. World Health Organization definition of myocardial infarction: 2008–09 revision. *Int. J. Epidemiol.* **2010**, *40*, 139–146. [[CrossRef](#)] [[PubMed](#)]
- Bax, L.; Algra, A.; Willem, P.T.M.; Edlinger, M.; Beutler, J.J.; van der Graaf, Y. Renal function as a risk indicator for cardiovascular events in 3216 patients with manifest arterial disease. *Atherosclerosis* **2008**, *200*, 184–190. [[CrossRef](#)] [[PubMed](#)]
- Avila, K.; Sanmartin, P.; Jabba, D.; Jimeno, M. Applications Based on Service-Oriented Architecture (SOA) in the Field of Home Healthcare. *Sensors* **2017**, *17*, 1703. [[CrossRef](#)] [[PubMed](#)]
- Sendra, S.; Parra, L.; Lloret, J.; Tomás, J. Smart system for children’s chronic illness monitoring. *Inf. Fusion* **2018**, *40*, 76–86. [[CrossRef](#)]
- Lloret, J.; Parra, L.; Taha, M.; Tomás, J. An architecture and protocol for smart continuous eHealth monitoring using 5G. *Comput. Netw.* **2017**, *129*, 340–351. [[CrossRef](#)]
- Lacuesta, R.; Garcia, L.; García-Magariño, I.; Lloret, J. System to recommend the best place to live based on wellness state of the user employing the heart rate variability. *IEEE Access* **2017**, *5*, 10594–10604. [[CrossRef](#)]
- Ramirez-Alaminos, J.M.; Sendra, S.; Lloret, J.; Navarro-Ortiz, J. Low-cost wearable bluetooth sensor for epileptic episodes detection. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
- Palatini, P.; Casiglia, E.; Julius, S.; Pessina, A.C. High heart rate: A risk factor for cardiovascular death in elderly men. *Arch. Intern. Med.* **1999**, *159*, 585–592. [[CrossRef](#)] [[PubMed](#)]
- Cook, S.; Togni, M.; Schaub, M.C.; Wenaweser, P.; Hess, O.M. High heart rate: A cardiovascular risk factor? *Eur. Heart J.* **2006**, *27*, 2387–2393. [[CrossRef](#)] [[PubMed](#)]
- Gupta, M.S.D.; Patchava, V.; Menezes, V. Healthcare based on IoT using Raspberry Pi. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, India, 8–10 October 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 796–799.
- Pretz, J.B.; da Costa, J.P.C.; Alvim, J.R.; Miranda, R.K.; Zanatta, M.R. Efficient and low cost MIMO communication architecture for smartbands applied to postoperative patient care. In Proceedings of the 2017 Second Russia and Pacific Conference on Computer Technology and Applications (RPC), Vladivostok, Russia, 25–29 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.
- Lee, M.; Lee, K.; Shim, J.; Cho, S.j.; Choi, J. Security threat on wearable services: Empirical study using a commercial smartband. In Proceedings of the IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Seoul, Korea, 26–28 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–5.
- Iancu-Constantin, R.; Serbanati, L.D.; Chera, C.; Gheorghe-Pop, I.D.; Ertl, B. An E-health approach for remote cardiac rehabilitation. In Proceedings of the 2015 20th International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 27–29 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 205–210.
- Nandkishor, B.R.; Shinde, A.; Malathi, P. Android smartphone based body area network for monitoring and evaluation of medical parameters. In Proceedings of the 2014 First International Conference on Networks & Soft Computing (ICNSC), Guntur, India, 19–20 August 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 284–288.

15. Hofer, T.; Schumacher, M.; Bromuri, S. COMPASS: An interoperable personal health system to monitor and compress signals in chronic obstructive pulmonary disease. In Proceedings of the 2015 9th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), Istanbul, Turkey, 20–23 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 304–311.
16. Rao, I.H.; Amir, N.A.; Dagale, H.; Kuri, J. e-SURAKSHAK: A cyber-physical healthcare system with service oriented architecture. In Proceedings of the 2012 International Symposium on Electronic System Design (ISED), Kolkata, India, 19–22 December 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 177–182.
17. Stevanoski, G.; Kocev, I.; Achkoski, J.; Koceski, S.; Temelkovski, B. Implementation of a System for Physiological Status Monitoring by using Tactical Military Networks. *Def. Sci. J.* **2016**, *66*, 517. [[CrossRef](#)]
18. García-Magariño, I.; Palacios-Navarro, G.; Lacuesta, R. TABSAOND: A technique for developing agent-based simulation apps and online tools with nondeterministic decisions. *Simul. Model. Pract. Theory* **2017**, *77*, 84–107. [[CrossRef](#)]
19. Moody, G.B.; Mark, R.G. A database to support development and evaluation of intelligent intensive care monitoring. In Proceedings of the 1996 Computers in Cardiology, Indianapolis, IN, USA, 8–11 September 1996; IEEE: Piscataway, NJ, USA, 1996; pp. 657–660.
20. García-Magariño, I.; Gonzalez Bedia, M.; Palacios-Navarro, G. FAMAP: A Framework for Developing m-Health Apps. In *World Conference on Information Systems and Technologies; Advances in Intelligent Systems and Computing*; Springer: Berlin, Germany, 2018; Volume 745, pp. 850–859.
21. Fortino, G.; Gravina, R.; Guerrieri, A.; Di Fatta, G. Engineering large-scale body area networks applications. In Proceedings of the 8th International Conference on Body Area Networks (BodyNets), Boston, MA, USA, 30 September–2 October 2013; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2013; pp. 363–369.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

6.5. ABS-DDoS: An agent-based simulator about strategies of both DDoS attacks and their defenses, to achieve efficient data forwarding in sensor networks and IoT devices.

Cita completa:




GONZÁLEZ-LANDERO, F., GARCÍA-MAGARIÑO, I., LACUESTA, R., & LLORET, J. (2018). ABS-DDoS: An Agent-Based Simulator about Strategies of Both DDoS Attacks and Their Defenses, to Achieve Efficient Data Forwarding in Sensor Networks and IoT Devices *Wireless Communications and Mobile Computing, 2018*.

Abstract:

Sensor networks and the Internet of Things (IoT) are useful for many purposes such as military defense, sensing in smart homes, precision agriculture, underwater monitoring in aquaculture, and ambient-assisted living for healthcare. Efficient and secure data forwarding is essential to maintain seamless communications and to provide fast services. However, IoT devices and sensors usually have low processing capabilities and vulnerabilities. For example, attacks such as the Distributed Denial of Service (DDoS) can easily hinder sensor networks and IoT devices. In this context, the current approach presents an agent-based simulation solution for exploring strategies for defending from different DDoS attacks. The current work focuses on obtaining low-consuming defense strategies in terms of processing capabilities, so that these can be applied in sensor networks and IoT devices. The experimental results show that the simulator was useful for (a) defining defense and attack strategies, (b) assessing the effectiveness of defense strategies against attack ones, and (c) defining efficient defense strategies with low response times.

Research Article

ABS-DDoS: An Agent-Based Simulator about Strategies of Both DDoS Attacks and Their Defenses, to Achieve Efficient Data Forwarding in Sensor Networks and IoT Devices

Franks González-Landero,¹ Iván García-Magariño ^{2,3},
Raquel Lacuesta ^{2,3} and Jaime Lloret ⁴

¹Edison Desarrollos, Teruel 44002, Spain

²Department of Computer Science and Engineering of Systems, University of Zaragoza, Teruel 44003, Spain

³Instituto de Investigación Sanitaria Aragón, Zaragoza, Spain

⁴Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universitat Politècnica de Valencia, Valencia, Spain

Correspondence should be addressed to Iván García-Magariño; ivangmg@unizar.es

Received 23 March 2018; Accepted 28 May 2018; Published 24 June 2018

Academic Editor: Wei Wang

Copyright © 2018 Franks González-Landero et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Sensor networks and Internet of Things (IoT) are useful for many purposes such as military defense, sensing in smart homes, precision agriculture, underwater monitoring in aquaculture, and ambient-assisted living for healthcare. Efficient and secure data forwarding is essential to maintain seamless communications and to provide fast services. However, IoT devices and sensors usually have low processing capabilities and vulnerabilities. For example, attacks such as the Distributed Denial of Service (DDoS) can easily hinder sensor networks and IoT devices. In this context, the current approach presents an agent-based simulation solution for exploring strategies for defending from different DDoS attacks. The current work focuses on obtaining low-consuming defense strategies in terms of processing capabilities, so that these can be applied in sensor networks and IoT devices. The experimental results show that the simulator was useful for (a) defining defense and attack strategies, (b) assessing the effectiveness of defense strategies against attack ones, and (c) defining efficient defense strategies with low response times.

1. Introduction

Sensor networks (SNs) are becoming useful in a large variety of sensing applications. One of these application is to monitor crop fields to irrigate and fumigate some specific areas when necessary [1]. In addition, underwater SNs are useful for assessing amounts of fish in fish farms [2]. This can be useful for delivering the right amount of food for properly feeding fishes in aquaculture without generating unnecessary food wastage. SNs can also be useful for military tactics [3]. In addition, Internet of Things (IoT) is useful for improving lifestyles, automating services, and making more information available in real-time. For example, IoT can be useful for providing the appropriate healthcare of patients when sleeping by means of smart beds [4]. In addition, IoT is also useful for improving the performance of waste collection considering risky material, in smart cities [5].

In general, efficient data forwarding is one of the key features of SNs and IoT devices. However, this efficiency can be hindered by external attacks. Cyber-crimes can provoke damage to normal citizen, companies, and even states. Cyber security measures are necessary to prevent these attacks. A common attack is the Distributed Denial of Service (DDoS) [6]. This attack consists in performing a high number of petitions to a service provider including a sensor or an IoT device, from machine multiples in order to make the target overloaded. There are several ways of performing this attack. The way most common way is to use botnets [7]. Botnets are infected machines whom owners do not know that they are part of an attack. Like in other technological aspects, cyber-attacks are continuously evolving and it is hard to predict what will be the future trends. IoT may cause an increase of infected devices numbers [8]. It is only enough to infiltrate a

harmful agent in a device and without the user knowing. The device may send information about its owner to other sites or the device may self-involve in a DDoS attack. The damage that these attacks can produce are well-known, such as millionaire losses, making an online service inaccessible, and damaging corporate image of a company. This damage motivates the improvement of cyber security techniques. In the context of SNs and IoT normally the processing capabilities are low, and consequently these techniques should be efficient.

The literature also includes both (a) works that focus on specific repercussions of DDoS, and (b) more general approaches that cover DDoS among other attacks. For example, the DDoS attack can be intended to meltdown a data center. In particular, [9] simulated this kind of attack, in which DDoS could be combined with problems/attacks in ventilation or air condition. Hence, this simulator focused on the specific repercussion on heating from DDoS attacks. In a more general context, [10] presented a multilayer approach that defended from multiple kinds of attacks, including DDoS. It exploited the complementary features among different filters obtaining a hybrid approach with low redundancies. However, those works did not provide a mechanism for defining and simulating strategies of DDoS attacks based on different mechanisms of coordination, as the current work does. Those works neither provided the possibility of determining and assessing defense strategies from DDoS attacks, while the current approach supported this possibility.

DDoS attacks can be prevented by defining lightweight algorithms that determine whether a request is real or faked. For example, a lightweight algorithm was defined for protecting controllers and switches in software-defined networks (SDNs) from DDoS attacks [11]. This algorithm was based on the analysis of the packets sent to a SDN and performed significantly better for SDN ecosystems of mobile users.

In this context, the current approach addresses the definition and assessment of both cyber-attacks and cyber-defenses, in order to estimate the cyber-defense's effectiveness when a SN node or a IoT device is attacked in different manners. More concretely, the current approach mainly focuses on the different strategies for performing and defending from DDoS attacks. In this work, we present the novel agent-based simulator (ABS) called ABS-DDoS. This simulator allows engineers to define strategies for performing attacks in different coordinated ways. It also allows engineers to define strategies for estimating which are the attackers in order to deny them the services and consequently being able to provide services the real requests. The current simulator assesses these strategies by simulating these together and providing such as the percentage of real requests that are successfully attended.

2. Materials and Methods

The main material of the current work is the novel simulator about DDoS attacks in sensors and IoT devices called ABS-DDoS, which is presented in Section 2.1. In addition, Section 2.2 describes the strategies that we have defined

The screenshot shows the main configuration screen of the ABS-DDoS simulator. It features a light blue background with a white title bar at the top containing the text 'ABS-DDoS'. Below the title bar, there are five rows of input controls. Each row consists of a label on the left and a corresponding input field on the right. The first row is 'Number of Malware Agents:' with a text box containing '225'. The second row is 'Number of Honest Agents:' with a text box containing '75'. The third row is 'Duration of simulation (hours):' with a text box containing '100'. The fourth row is 'Attacker strategy:' with a dropdown menu showing 'Coordinated Fixed'. The fifth row is 'Defense strategy:' with a dropdown menu showing 'Coordinate Defense'. At the bottom center of the screen, there is a rectangular button labeled 'Run Simulation'.

FIGURE 1: Main screen of the application.

with ABS-DDoS for the current experiments. Furthermore, Section 2.3 introduces the procedure that we have followed to assess the utility of this novel simulator in improving the security regarding DDoS attacks.

2.1. ABS-DDoS: An ABS of Strategies for Both Performing and Defending from DDoS Attacks. ABS-DDoS is a simulator about DDoS attacks. It is implemented as an ABS, in which sensor and IoT devices are modeled as agents providing services. Other agents coordinately perform DDoS attacks. ABS-DDoS allows users to define and simulate several strategies about DDoS attacks. It also allows users to define defense strategies and simulate their results when defending from certain strategies of DDoS attacks.

Figure 1 presents the main screen of the user interface (UI) of the simulator. This input screen allows users to set the input parameters for simulations, which are (1) number of malware agents, (2) number of honest agents, (3) duration of simulation, (4) attacker strategy, and (5) defense strategy. The first parameter is the number of malware agents and their role is to simulate bots' attacks against a server. The second parameter is the number of honest agents, which simulate requests made by normal users. The third parameter is duration of simulation in h and represents the number of iterations in the simulation. Finally, the last parameters represent attack/defense strategies that users can use in simulations. When a user finalizes setting up all input parameters, they can press "Run Simulation" button to start a simulation.

Figure 2 depicts the whole app functionality. The tool has four main agent types. The simulation entails a periodic execution with several cycles. The number of cycles is established by the duration parameter in the simulation. For instance, if a user sets a duration value of 25, it means that each agent has the possibility of taking autonomous decisions 25 times. Agent subtypes share similar characteristics but

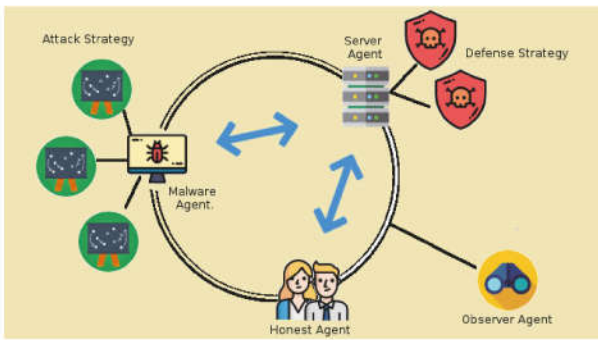


FIGURE 2: Overview of the strategy system.

they can have their own behaviors. The simulator creates all agents then adds them to simulation and finally executes each agent. The server agent simulates a machine whose function can be to give services, to response to queries, or to forward data. Moreover, server agent represents the target machine that malware agents will attack. The agent server has a certain strategy defense established by the defense strategy parameter. The defense strategy indicates how a server agent defends itself from attacks of malware agents. The malware agent simulates each machine that may perform DDoS attacks. Each malware agent subtype has a certain attack strategy and it describes how to perform attacks against a server agent. Attacks may be in waves, during an elapsed time or coordinated.

The third main agent type is honest agents. These agents represent normal users, SN nodes, or IoT devices that perform legitimate requests to the server agent. The decisions of honest agents about whether requesting services is simulated using a low and configurable value. In particular, we simulated these nondeterministic decisions using the principles of TABSAOND (a technique for developing agent-based simulation apps and online tools with nondeterministic decisions) [12]. A random number is generated in the $[0, 1)$ interval, and it is compared with the probability. If the number is lower than the probability, then the honest agent requests a service to the server agent.

It is worth mentioning that each server agent has a limited number of requests that can be attended per iteration. If the limit is reached, this agent will mandatorily deny all the remaining requests in the corresponding iteration.

The last agent type is observer agent. The main function of this agent is to collect data about simulations. Specifically, it gives us information such as percentage of success of honest agent, percentage of success attackers, and percentage of success of customers in each of iteration. All this information is saved into a file, so we were able to further analyze if after the simulation.

ABS-DDoS was developed with Unity 5.6.1f1. Unity game-based engine is popular and well-known among developers' community. Unity is popular because it is multiplatform, allowing the deployment of applications in several operative systems, typing code only once. We used Unity because it offers a suitable environment in order to work with the Process for developing Efficient Agent-Based Simulators

(PEABS) [13]. The underlying framework of PEABS was made for being used with Java, Unity, and Apache Cordova, and it has several methods to create agents and their behaviors. Thanks to Unity and PEABS, we have built a suitable environment for simulating strategies of attacks and defenses.

We selected PEABS instead of other agent-oriented methodologies because it combined short development time, technological support for software development, and high performance of the resulting systems in the particular case of ABSs. For instance, other theoretical methodologies such as the Gaia agent-oriented methodology lacked technological support for development, and other practical methodologies like Ingenias generated less efficient systems. In addition, we used the framework of PEABS instead of other well-known agent-oriented frameworks such as the Java Agent Development Framework (JADE), because PEABS allowed one to develop more efficient systems in the specific case of ABSs.

The definition of strategies is different between attack and defense strategies. For defining an attack strategy, users must create a new class that inherits from "MalwareAgent" class. This class must overwrite the Live method. Users can define fields for storing or analyzing any information. The Live method can call "AskService" to simulate the requests of services. The objects of this class should coordinate to ask services simultaneously in specific simulation iterations to achieve that the service is denied to honest agents.

To define a new defense strategy, users implement a new class that inherits from "ServerAgent". This class should overwrite the "DecideWhetherToProvideService" method for defining the reactive behaviors. It can also overwrite the Live if it needs to take any proactive action per iteration. The reactive behavior occurs when the strategy must react to certain event. In this case, the strategy reacts at the moment when a customer asks for a service. The implementation of the DecideWhetherToProvideService is normally the core of the new defense strategy. This method should decide whether to provide the service to this sender, by only knowing which is identifier. The strategy can use new class fields to store and analyze the history of requests of each agent ID. The implementation of the Live method is useful for performing any operation that needs to be taken only once per iteration or is related to the analysis of the collective behavior.

2.2. Strategies Defined with ABS-DDoS. Following the current approach with ABS-DDoS, we have defined the attacking strategies: (a) Coordinated Fixed Interval Attacker Agent, (b) Half-and-Half Attack, and (c) Substitute Attack. In addition, we have defined the defense strategies Frequency Defense and Coordinate Defense Server Agent.

2.2.1. Coordinated Fixed Interval Attack. In the strategy Coordinated Fixed Interval Attack (CFIA), all the attacker agents are coordinated to attack together periodically in a shared fixed interval.

As one can see in the diagram of Figure 3, all malware agents are waiting for an attack moment. In each step, they check the iteration number representing the time stamp. If

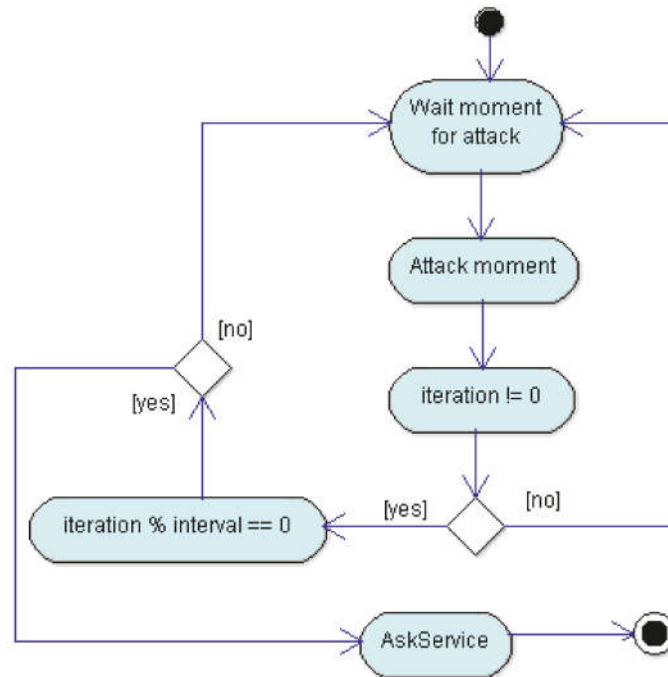


FIGURE 3: Coordinated fixed interval strategy.

the iteration is the first one, they will do nothing and keep waiting. If malware agents are not on their first iteration, they will check the attack moment. The attack moment is based on a fixed interval of iterations, and this interval can be set up by the user. For instance, if the simulation has 25 iterations in whole and user has set the interval to 5, then malware agents will attack 5 times during the whole simulation. Finally, the malware agents calculate this moment by calculating the remainder of dividing the iteration number and fixed interval. If the result is 0, malware agents will attack. Otherwise, they will keep waiting for another attack moment.

2.2.2. Half-and-Half Attack. The Half-and-Half (HaH) strategy is aimed at making its behavior more difficult to be detected than CFIA. Half-and-half attack is a natural evolution of CFIA. In this strategy, only half of the malware agents perform the requests in a certain iteration, and the other remaining half perform the requests in the other attack moments. In the diagram of Figure 4, one can see how HaH strategy works. Like in CFIA server agent is waiting for the attack moment and then it checks whether it is not in first iteration and it is in a suitable iteration (it means the iteration must match with the fixed interval set up by the user). Then, the agent decides whether it should attack. For this purpose, the agent determines whether the current iteration number is even or odd. Each agent has an integer ID number. In each even iteration, the strategy provokes that malware agents with even ID number request services to the target server agent. In each odd iteration, malware agents with odd ID number will send requests. Finally, when each malware agent knows if it is in even or odd iteration, it asks service. For instance, if our simulation has 25 iterations and 100 malware agents, in iteration number 5, 50 malware agents will attack server

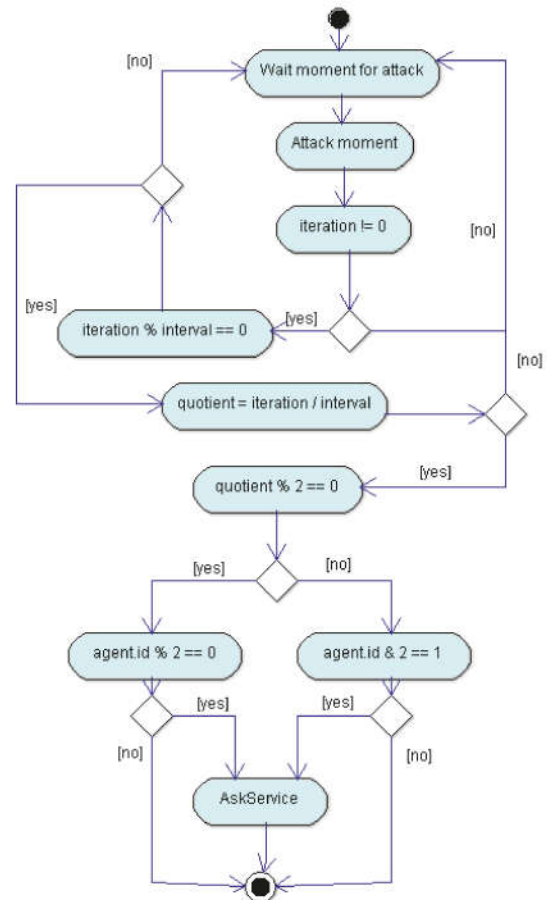


FIGURE 4: Strategy half and half.

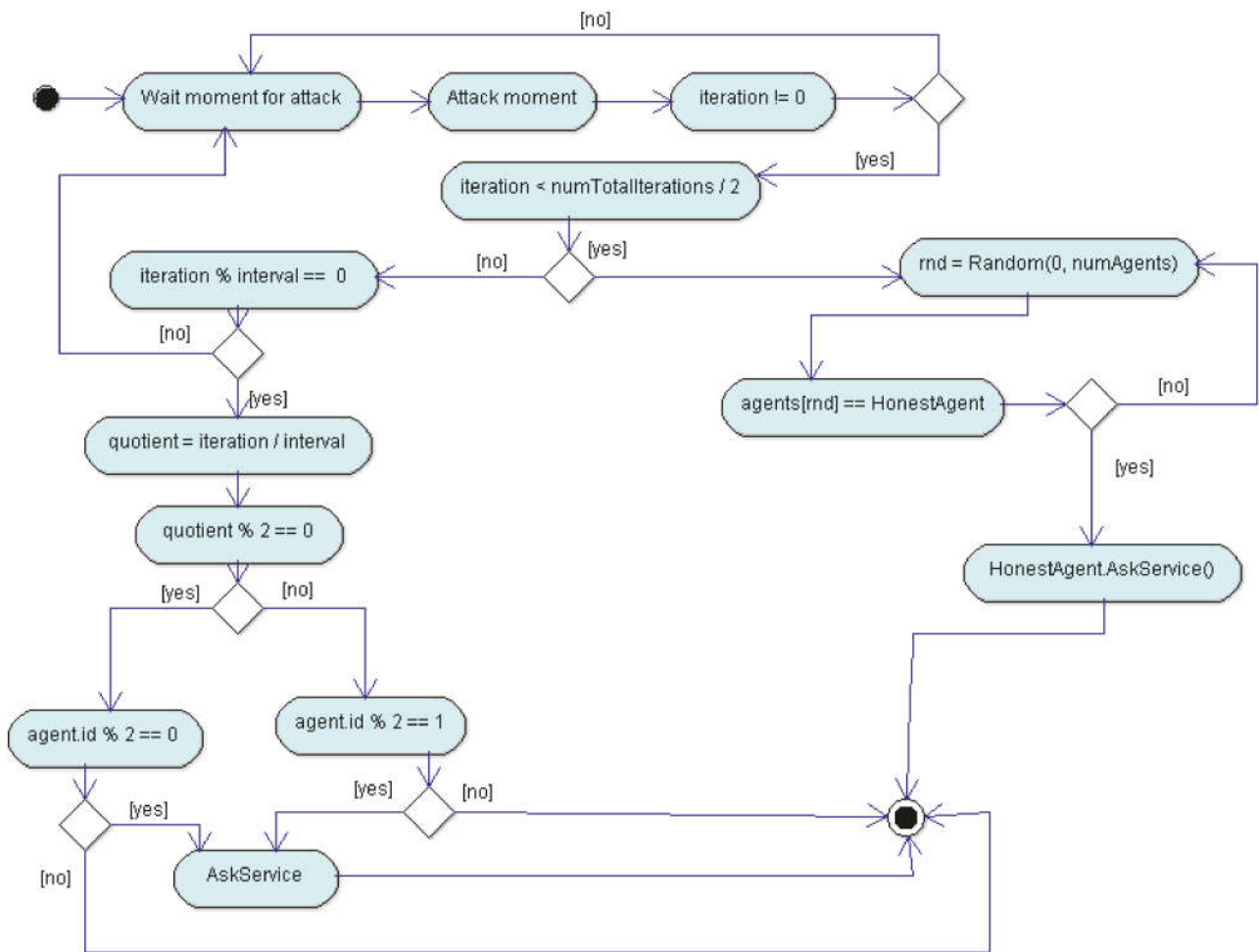


FIGURE 5: Substitute attack strategy.

agent. The next attack it will be in iteration number 10, but they will be the other remaining 50 malware agents.

2.2.3. Substitute Attack. Substitute Attack (SA) simulates the interception of encrypted messages and forwarding these. The purpose is to overload the target server agent, although these messages of requests may not be necessarily addressed to the target agents. The advantage of this attack is that the few successful forwarded messages that can actually be redirected to the same service use the identifier of a different agent. Thus, these are more difficult to be tracked. This attack would use the well-known man-in-the-middle attack [14] to acquire these message.

This attack follows two phases. The functionality can be seen in the diagram in Figure 5. In the first phase, this chooses a random agent from the ones that have requested the service. Then, it checks if the agent selected is an honest agent (by checking whether it is not one of the fellow attacker agents). If selected agent is not honest agent, the malware agent chooses other agents randomly until he catches an honest agent. When an honest agent is selected, a malware agent asks a service as if it was this honest agent. In this way, malware agents may saturate a server agent faster and the latter may deny real service requests in the next iterations.

On the other hand, the second phase of this strategy occurs in simulation's second half. In this second phase, malware agents attack normally; it means that they execute their own method "AskService". Moreover, in the second phase malware agents use HaH strategy in the same way as it was explained in the previous section.

2.2.4. Frequency Defense. Frequency Defense (FD) has like a main aim detecting agent's frequency on asked a service. If FD detects a high frequency it will not give service a certain agent. In order to determine whether an agent has a high frequency, FD measures the percentage of iterations in which it requests a service. If this agent requests services over a certain threshold, FD will deny to give a service. The aforementioned threshold is defined as an internal parameter. When this agent is created, the FD creates an index about the number of requests from each requester agent (unknown either malware or honest agent). In this way, Server Agent can save the absolute frequency of each agent. Then this frequency is divided by the number of iterations to obtain a relative frequency.

The reactive behavior of defense strategies is defined in "DecideWhetherToProvideService". In this method, a defense strategy decides whether to provide service regarding

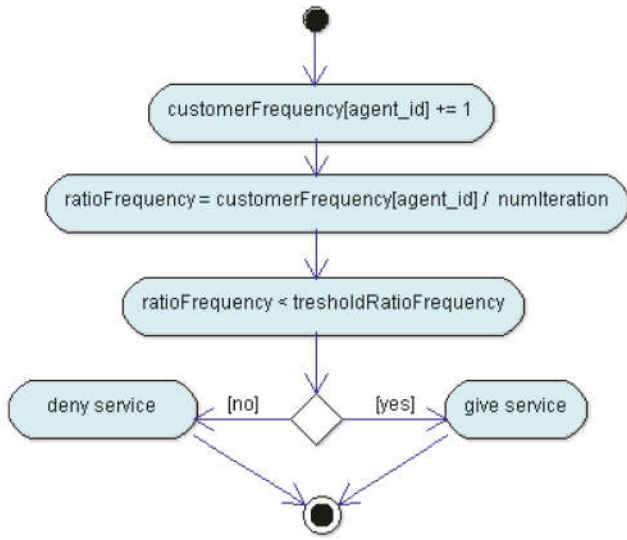


FIGURE 6: Strategy frequency server agent.

its estimation about whether the request was made by a malware agent.

Figure 6 depicts the process about how FD decides whether to provide a service or not. Each time a server agent receives a request, it updates its frequency record about the sender identified by its ID, including its absolute frequency and its frequency per time unit. The latter frequency is calculated as follows:

$$f_t(x) = \frac{f(x)}{(I_n + 1)} \quad (1)$$

where $f_t(x)$ is the frequency of requests of agent x per time unity, $f(x)$ determines the absolute frequency of agent x , and $I_n + 1$ determines the number of iteration (representing the number of hours simulated up to current state of the simulation).

Finally, if the frequency per time unit is lower than a parametric internal threshold, Server Agent will provide service to this agent. Conversely, if this frequency is greater than the threshold, Server Agent will not provide service.

2.2.5. Coordinated Defense. The main goal of Coordinate Defense (CD) is to detect when it has been attacked by strategies with patterns similar to CFIA. Since this strategy is more complex than FD, we are going to explain it in three phases: Constructor Phase, Decide Phase, and Perform Phase. Constructor Phase occurs when the simulator runs CD's constructor. In constructor phase, CD sets up all initial parameters and initial variables. On the one hand we have two vectors, one of them will count all requests made by agents in only one iteration, and the other of them will count all requests made by agents in whole simulation. A request threshold is assigned to a product of the maximum amount of services given in one iteration and the ratio of frequency threshold. Both variables are established with arbitrary value given by programmer. The request threshold is defined with the following equation:

$$t = S_{max} * R \quad (2)$$

where t is request threshold, S_{max} is the max number of services that can be provided per iteration, and R is the ratio threshold request.

In addition, it initializes a counter for counting the number of requests the server agent. In this strategy, if the number of requests surpasses the requests thresholds, the server agent will assume that it is being attacked.

The second phase, Decide Phase, occurs when CD has to decide whether to provide a service. Figure 7 shows the flow diagram of this phase. In this diagram, one can see all the process inside the overwritten method "DecideWhetherToProvideService". Each time an agent asks a service, CD counts it as like as FD and then increases the variable that represents the number of requests in an iteration. Until this point is similar to FD, from this point the process changes. CD checks whether it has been attacked. If it has not been attacked, it gives service. If CD has been attacked previously, CD calculates the ratio of requests in attacks. It is calculated as quotient between (a) the amount of requests that a certain agent has made in all the requests in iterations identified as attacks and (b) the number of these iterations identified as attacks. Finally, ratio request in attack is compared with threshold frequency in attack. The threshold frequency in attack is an internal parameter different from the one previously presented. It represents the barrier for discriminating the estimation between real requests and fake ones, based on how frequently an agent performs requests when DDoS attacks are detected. If the ratio request in attack of an agent surpasses this threshold, CD denies the service to this agent.

The final phase, the Perform Phase, occurs when CD agent has its turn for performing proactive actions. This is implemented overriding the "Live" method as instructed by PEABS. When the simulator finishes creating all agents, then it commands all agents to execute their own inherited method "Live". The first agents that execute this method are malware agents and honest agents. Then, CD executes this method. In method "Live". CD compares the amount of requests that has received only in current iteration with the threshold of requests. If the amount of requests is greater than the threshold of requests, it increases the total counter of attacks ("numAttacksTotal" in the diagram of Figure 7). In this case, it also updates index about the amount of times that each agent asks a service in the iterations identified as attacks (referred as "totalRequestInAttack" in the diagram), using the record about the number of times each agent asked a service during the current iteration (denoted as "currentRequest"). Finally, in all the iterations regardless whether an attack was detected, the currentRequest is reset to zero times for each agent; the counter of the requests in the current iteration (referred as "numRequestInAIteration") is also reset to zero.

2.3. Method of Conducting the Experiments. We were alternatively defining attack and defense strategies. Each attack was aimed at exploiting the vulnerabilities of the previous defense. Each defense was aimed at protecting from the previous attack.

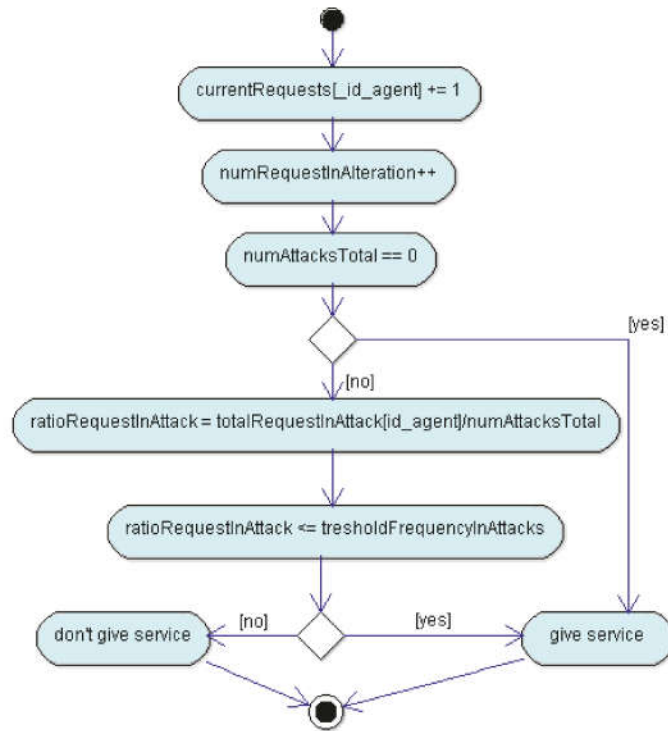


FIGURE 7: Strategy Coordinate Defense Server Agent.

TABLE 1: Simulated combinations of attack and defense strategies.

Defense Strategy	Attack Strategy
Frequency Defense	Half and Half Attack
Frequency Defense	Substitute Attack
Frequency Defense	Coordinated Fixed Interval Attack
Coordinated Defense	Half and Half Attack
Coordinated Defense	Substitute Attack
Coordinated Defense	Coordinated Fixed Interval Attack

The first simple attack was a continuous requester. The first defense was FD. From this point forward, we developed the strategies that we introduced in Section 2.2.

Then, we analyzed all the possible combinations of defense and attack strategies from the ones described in Section 2.2. Table 1 shows the combinations that we tested.

For the observation, we analyzed a short interval of the simulated time (25 h), to understand the periodic behavior. We also analyzed long interval to observe the evolution in the long term (100 h). In all the experiments, we used 100 malware agents and 30 honest agents.

In order to assess the performance of the most advanced defense strategy, we executed each with the most advanced attack strategy (i.e., SA). We performed several tests increasing, respectively, the number of agents performing requests and the simulated time.

3. Results and Discussion

Figures 8 and 9 show evolution results of simulating CFIA attacks on an agent defending with FD strategy. FD has



FIGURE 8: FD versus CFIA, simulation evolution of 25 h.

a vulnerability that CFIA can exploit. CFIA can reduce its frequency of requests by decreasing its frequency of coordinated attacks. In this way CFIA agents may not be detected by FD strategy.

The success of attackers is low, probably because the number of attackers is much higher than the number of possible services per iterations. Thus, only a few attackers get the service.

CFIA strategy achieve a successful DDoS, because customers only succeeded 50% in average. In addition, the results of the customer success per hour is the most evident fact that the DDoS attacks succeeded, since this measure indirectly revealed the proportion of denials to real service requests. The customer success per hour decreased to zero or almost zero in the specific hours where DDoS was executed.

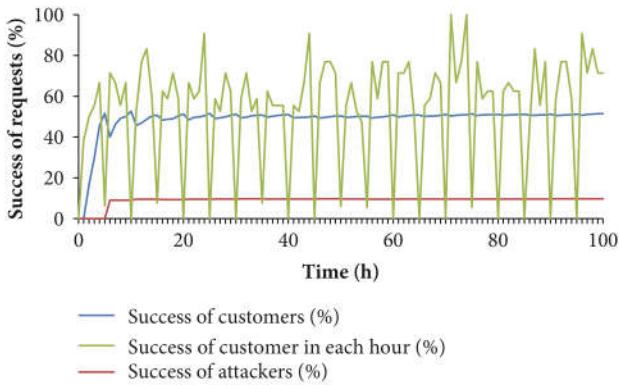


FIGURE 9: FD versus CFIA, simulation evolution of 100 h.

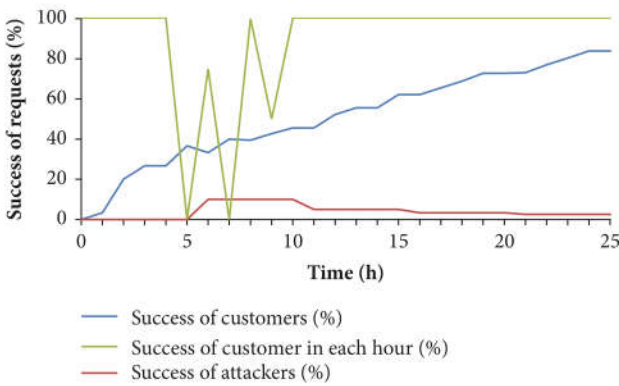


FIGURE 10: CD versus CFIA, simulation evolution of 25 h.

The beginning of the global success of customers started with low a value because of the first attack was conducted in the first iteration. This value increased when this average measure was compensated in the in-between iterations without attacks.

The success of attackers is low because there are much more attackers than services the server agent can provide. However, the relevant measure of DDoS success is to achieve the fact that the service is denied to most customers.

Figures 10 and 11 show evolution examples of simulating CFIA attacks to CD strategy.

In fifth hour (the first attack), the attackers were not detected because they have not been tracked, and moreover, it is the first attack. Therefore, someone of them had success (10%). As the simulation progressed, in the next attacks, the attackers were well tracked; therefore the percentage success is going down near 0 after simulating 100 h.

Some of the honest agents were misclassified as attackers, and therefore at the next iterations they were discriminated. For this reason, one can see the percentage of customer success going down. In the second attack (after simulating 10 h), we can see that the relative amount of misclassified honest agents decreased. It is improbable that two honest agents asked a service in two different moments of attack. Specifically, the probability that an agent asks a service is 10%. Therefore, the probability of the same agent asks a service in

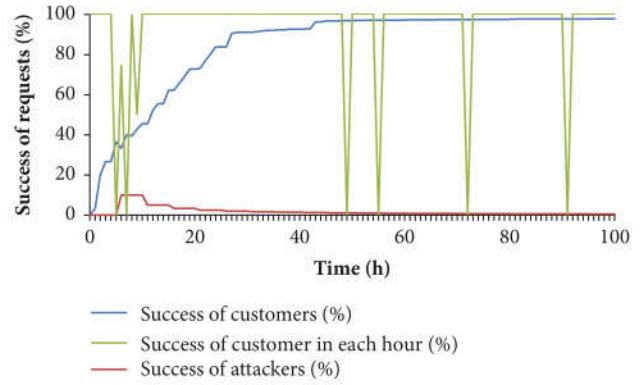


FIGURE 11: CD versus CFIA, simulation evolution of 100 h.

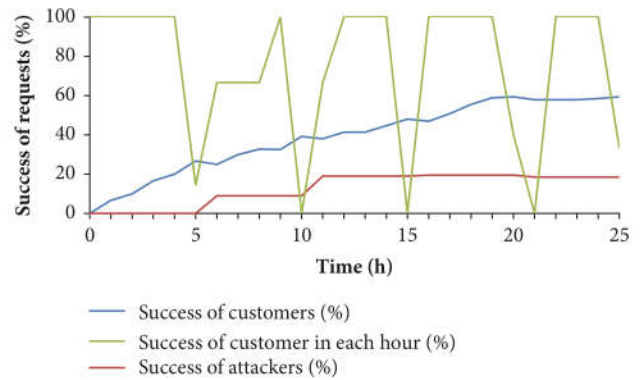


FIGURE 12: CD versus HaH, simulation evolution of 25 h.

the two first attacks is 0.01 (0.1×0.1), and the probability of asking in the three first attacks is 0.001 (0.1^3) and so on.

After simulating 45 h, sometimes the customer success per hour decreased to zero. The reason is probably that in these interactions none honest agent performed a request, and then the measure outputted the zero default value when avoiding raising the exception of division by zero.

Figures 12 and 13 show the results of performing attacks following HaH strategy to the defense following CD strategy. One can observe that HaH is more difficult to be tracked than CFIA, since in this strategy the attacks are not always performed by the same agents. The DDoS were successful since in most attacks, the customer success per hour reduced to zero. In addition, the global success of attackers was relatively high (around 20%). Since only the half of the attackers were used, a lower number of requests were denied for both honest and malware agents.

Figures 14 and 15 show the simulation of the combination of HaH attack strategy and FD defense strategy. FD defense is much more flexible in detecting attacks by frequencies, as it considers all the iterations and not only the ones suffering attacks. Hence, all the DDoS attacks successfully achieved the denials of services to honest agents, as one can observe in the decreases to zero or near-to-zero values in the attack iterations.

Figures 16 and 17 show simulation evolution examples of SA attacks and FD defenses, while Figures 18 and 19 show

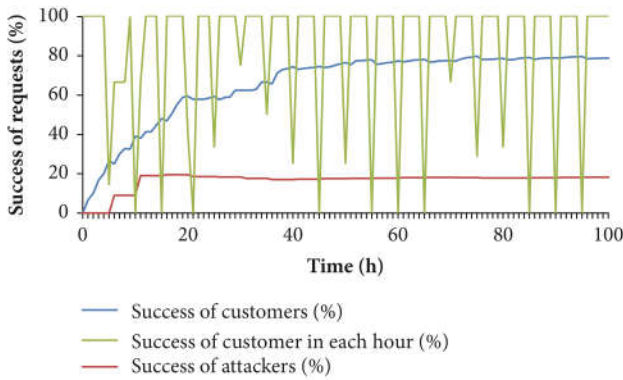


FIGURE 13: CD versus HaH, simulation evolution of 100 h.

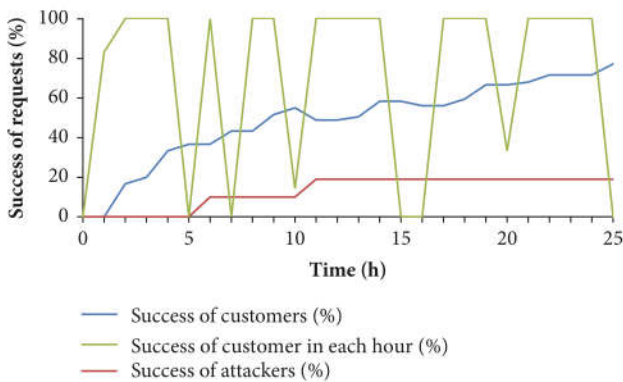


FIGURE 14: FD versus HaH, simulation evolution of 25 h.

simulation evolutions of SA attacks and CD defenses. SA was effective for exploiting the vulnerabilities of both defense strategies. The reason is that the impersonation of some honest agents make them look like attackers to both defense strategies. Thus, the success of customers per hour decreased not only in the attacked iterations but also in the others.

In Figure 19, in the middle of the simulation (i.e., about 50 h of simulation), one can observe a different behavior in the success of customers. In the second phase the success of customers do not depend on the possibility of being able to apply man-in-the-middle.

Although, SA seems to be the most effective attack theoretically, it depends on the ability of finding and impersonating other honest agents requesting a specific service.

Figures 20 and 21 show the response times in deciding whether to provide service for each request of the CD defense strategy when trying to defend from SA attack. One can observe that the average response time does not increase when augmenting the simulation duration. Thus, this defense strategy could probably run continuously without losing defense. By contrast, the time response for deciding whether to provide service increases when increasing the number of agents performing requests to a given service. However, the response times had a low absolute value. In addition, both FD and CD have a constant computational costs since the records and indexes can be accessed and updated in constant computational cost. Therefore, the current approach

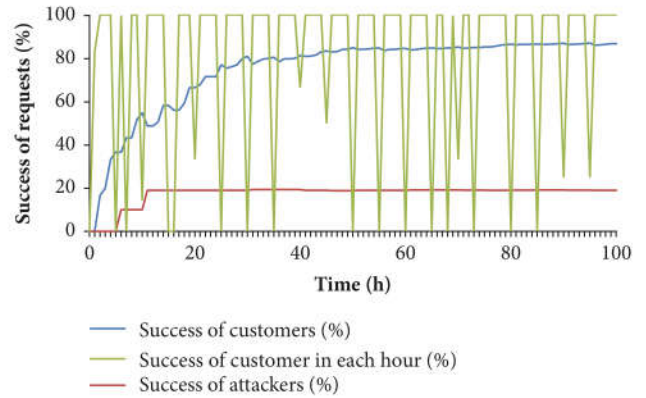


FIGURE 15: FD versus HaH, simulation evolution of 100 h.

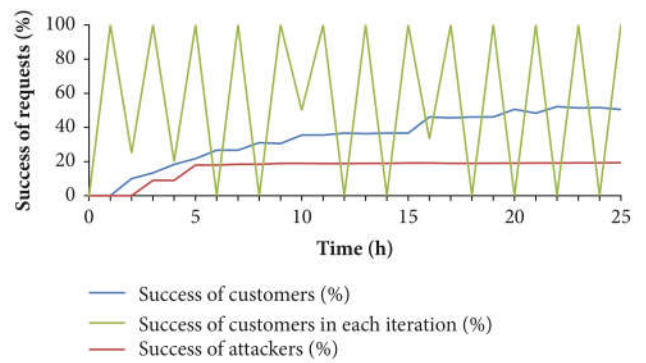


FIGURE 16: FD versus SA, simulation evolution of 25 h.

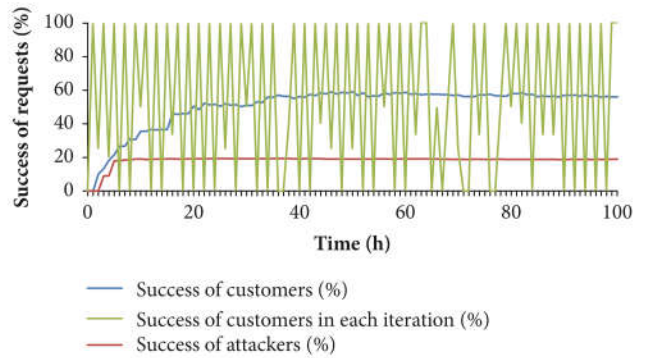


FIGURE 17: FD versus SA, simulation evolution of 100 h.

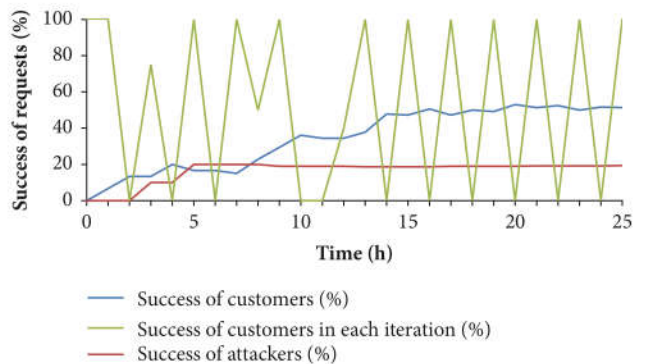


FIGURE 18: CD versus SA, simulation evolution of 25 h.

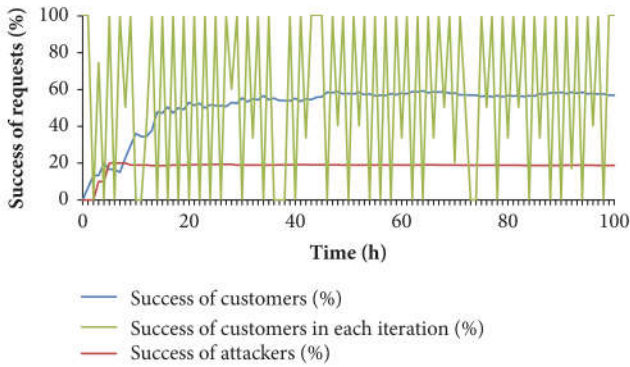


FIGURE 19: CD versus SA, simulation evolution of 100 h.

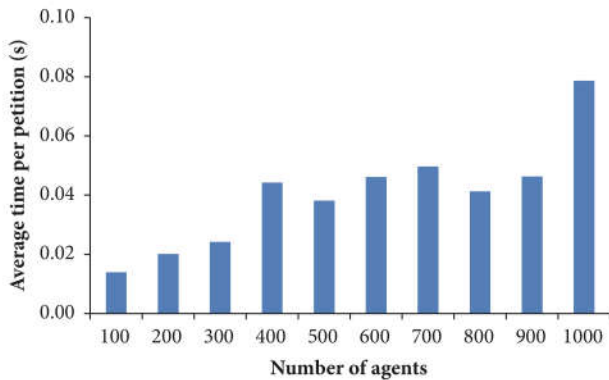


FIGURE 20: CD versus SA, response times when increasing the number of agents.

is efficient enough to be applied in SN sensors and IoT devices for performing efficient data forwarding or other services.

4. Conclusion and Future Work

The current work has presented a mechanism for improving security concerning DDoS attacks, by allowing developers to easily define and assess both attack and defense strategies in this context. The current approach also allows detecting DDoS security challenges by defining DDoS attack strategies that are usually to track for being counteracted. The current approach is based on the novel ABS called ABS-DDoS. We have defined and assessed two defense strategies and three attack strategies with ABS-DDoS. This ABS helped us to understand the results of all the possible combinations. In addition, we defined defense strategies that were efficient in terms of time response for deciding whether to provide services. In this way, these strategies can be used for maintaining security in SN sensors and IoT devices with low processing capabilities from DDoS attacks.

The proposed ABS is planned to be extended in order to simulate other types of attacks such a man-in-the-middle and zero-day attack. This may require define new agent types that will allow defining defense and attack strategies for attacks like man-in-the-middle attack or zero-day attack. These agent types would need to incorporate and manage the necessary

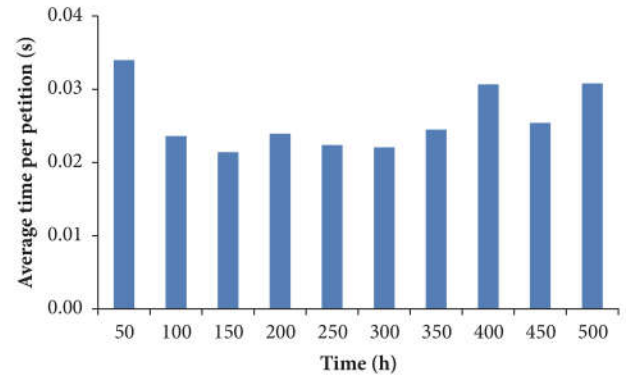


FIGURE 21: CD versus SA, response times when increasing the number of simulated hours.

information for measuring the effectiveness of defense and attack strategies in the context of each security attack. For example, in the case of the man-in-the-middle, a metric could be the percentage of messages that have successfully intercepted and forwarded.

Moreover, we plan to deploy advanced defense and attack strategies in real scenarios. We plan to test some attack strategies in SNs and IoT devices to exploit their vulnerabilities. Then, we will install defense strategies in SN sensors and IoT devices to protect from these attacks, in order to measure response times and effectiveness of the defense strategies in these devices with low processing capabilities. We also plan to test defense and attack in cloud services, which are one of the most frequent target nowadays, according to [15]. If we have the chance, we can test in important websites such as the ones from any government or big company. Finally, we could organize security contexts in which participants define defense and attack strategies with ABS-DDoS and compete against each other by means of the simulator.

Data Availability

All the relevant data of the current work are mentioned in the article or shown in its graphs.

Conflicts of Interest

The authors declare that there are not any conflicts of interest about the current work.

Acknowledgments

The authors acknowledge the research project “Construcción de un Framework para Agilizar el Desarrollo de Aplicaciones Móviles en el Ámbito de la Salud” funded by University of Zaragoza and Foundation Ibercaja with Grant Reference JIUZ-2017-TEC-03. This work has been supported by the program “Estancias de Movilidad en el Extranjero José Castillejo para Jóvenes Doctores” funded by the Spanish Ministry of Education, Culture and Sport with Reference CAS17/00005. The authors also acknowledge support from

“Universidad de Zaragoza”, “Fundación Bancaria Ibercaja”, and “Fundación CAI” in the “Programa Ibercaja-CAI de Estancias de Investigación” with Reference IT1/18. This work acknowledges the research project “Desarrollo Colaborativo de Soluciones AAL” with reference TIN2014-57028-R funded by the Spanish Ministry of Economy and Competitiveness. It has also been supported by “Organismo Autónomo Programas Educativos Europeos” with Reference 2013-1-CZ1-GRU06-14277. Furthermore, they acknowledge the “Fondo Social Europeo” and the “Departamento de Tecnología y Universidad del Gobierno de Aragón” for their joint support with Grant no. Ref-T81.

References

- [1] H. M. Jawad, R. Nordin, S. K. Gharghan, A. M. Jawad, and M. Ismail, “Energy-efficient wireless sensor networks for precision agriculture: A review,” *Sensors*, vol. 17, no. 8, 2017.
- [2] I. García-Magariño, R. Lacuesta, and J. Lloret, “ABS-FishCount: An Agent-Based Simulator of Underwater Sensors for Measuring the Amount of Fish,” *Sensors*, vol. 17, no. 11, p. 2606, 2017.
- [3] S. H. Lee, S. Lee, H. Song, and H. S. Lee, “Wireless sensor network design for tactical military applications : Remote large-scale environments,” in *Proceedings of the MILCOM 2009 - 2009 IEEE Military Communications Conference*, pp. 1–7, Boston, MA, USA, October 2009.
- [4] I. García-Magariño, R. Lacuesta, and J. Lloret, “Agent-Based Simulation of Smart Beds With Internet-of-Things for Exploring Big Data Analytics,” *IEEE Access*, vol. 6, pp. 366–379, 2018.
- [5] T. Anagnostopoulos, K. Kolomvatsos, C. Anagnostopoulos, A. Zaslavsky, and S. Hadjiefthymiades, “Assessing dynamic models for high priority waste collection in smart cities,” *The Journal of Systems and Software*, vol. 110, pp. 178–192, 2015.
- [6] X. Yang, S. Zhou, G. Ren, and Y. Liu, “Computer network attack and defense technology,” *Information and Computer Security*, vol. 1, no. 1, pp. 35–41, 2018.
- [7] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfari, “Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art,” *International Journal of Computer Applications*, vol. 49, no. 7, pp. 24–32, 2012.
- [8] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “IoT POT: analysing the rise of IoT compromises,” *EMU*, vol. 9, pp. 1–9, 2015.
- [9] Z. Anwar and A. W. Malik, “Can a DDoS attack meltdown my data center? A simulation study and defense strategies,” *IEEE Communications Letters*, vol. 18, no. 7, pp. 1175–1178, 2014.
- [10] S. Huda, R. Islam, J. Abawajy, J. Yearwood, M. M. Hassan, and G. Fortino, “A hybrid-multi filter-wrapper framework to identify run-time behaviour for fast malware detection,” *Future Generation Computer Systems*, vol. 83, pp. 193–207, 2018.
- [11] C. Gkountis, M. Taha, J. Lloret, and G. Kambourakis, “Lightweight algorithm for protecting SDN controller against DDoS attacks,” in *Proceedings of the 2017 10th IFIP Wireless and Mobile Networking Conference (WMNC)*, pp. 1–6, Valencia, September 2017.
- [12] I. García-Magariño, G. Palacios-Navarro, and R. Lacuesta, “TABSAND: A technique for developing agent-based simulation apps and online tools with nondeterministic decisions,” *Simulation Modelling Practice and Theory*, vol. 77, pp. 84–107, 2017.
- [13] I. García-Magariño, A. Gómez-Rodríguez, J. C. González-Moreno, and G. Palacios-Navarro, “PEABS: a process for developing efficient agent-based simulators,” *Engineering Applications of Artificial Intelligence*, vol. 46, pp. 104–112, 2015.
- [14] A. Akhuznada, M. Sookhak, N. B. Anuar et al., “Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions,” *Journal of Network and Computer Applications*, vol. 48, pp. 44–57, 2015.
- [15] Q. Yan, F. R. Yu, Q. X. Gong, and J. Q. Li, “Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

Parte I

Apéndices

Apéndice A

Factor de impacto de las publicaciones

RESUMEN: La presente sección enumera todos los trabajos publicados para la elaboración de la presente tesis con su correspondiente factor de impacto. Además presenta la contribución del doctorando en el que aparece como coautor.

A.1. Trabajos en primera autoría

- González-Landero, F., García-Magariño, I., Amariglio, R., & Lacuesta, R. (2019). Smart Cupboard for Assessing Memory in Home Environment. *Sensors*, 19(11), 2552. (**JCR SCI 2019 3.275, percentile 77.344%, Q1**).
- González-Landero, F., García-Magariño, I., Lacuesta, R. & Lloret, J. (2018). PriorityNet App: A mobile application for establishing priorities in the context of 5G ultra-dense networks. *IEEE Access*, 6, 14141-14150 (**JCR SCI 2018 4.098, percentile 85.484%, Q1**).
- González-Landero, F., García-Magariño, I., Lacuesta, R. & Lloret, J. (2018). Green Communication for Tracking Heart Rate with Smartbands. *Sensors*, 18(8), 2652. (**JCR SCI 2018 3.031, percentile 76.230%, Q1**).
- González-Landero, F., García-Magariño, I., Lacuesta, R., & Lloret, J. (2018). ABS-DDoS: an agent-based simulator about strategies of both DDoS attacks and their defenses, to achieve efficient data forwarding in sensor networks and IoT devices . *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7264269, 11 pages, (**JCR SCI 2018 1.396, percentile 30.263%, Q3**).

A.2. Trabajos en coautoría

- García-Magariño, I., González-Landero, F., Amariglio, R. & Lloret, J. (2019). Collaboration of smart IoT devices exemplified with smart cupboards. *IEEE Access*, 7(1), 9881-9892 (**JCR SCI 2019 3.745, percentile 77.885%, Q1**).

En la publicación citada en el apartado A.2 titulada *Collaboration of smart IoT devices exemplified with smart cupboards* el doctorando se encargó de las funciones de construir el primer prototipo de armario inteligente. Además, fue el encargado de dirigir y coordinar la batería de experimentos entre aplicaciones y dispositivos IoT. Finalmente, en cuanto a la aportación del manuscrito, redactó la sección *V. Experimentation* del manuscrito citado.

Bibliografía

- ABRAS, C., MALONEY-KRICHMAR, D., PREECE, J. ET AL. User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*, vol. 37(4), páginas 445–456, 2004.
- ABROL, A. y JHA, R. K. Power optimization in 5g networks: A step towards green communication. *IEEE Access*, vol. 4, páginas 1355–1374, 2016.
- ABU-FARAJ, Z. O., JABBOUR, E., IBRAHIM, P. y GHAOUI, A. Design and development of a prototype rehabilitative shoes and spectacles for the blind. En *2012 5th International Conference on BioMedical Engineering and Informatics*, páginas 795–799. IEEE, 2012.
- AHMED, M. S., MOHAMED, A., HOMOD, R. Z., SHAREEF, H., SABRY, A. H. y KHALID, K. B. Smart plug prototype for monitoring electrical appliances in home energy management system. En *2015 IEEE Student Conference on Research and Development (SCOReD)*, páginas 32–36. IEEE, 2015.
- AHN, B.-G., NOH, Y.-H. y JEONG, D.-U. Smart chair based on multi heart rate detection system. En *2015 IEEE SENSORS*, páginas 1–4. IEEE, 2015.
- ALJEHANI, S. S., ALHAZMI, R. A., ALOUFI, S. S., ALJEHANI, B. D. y ABDULRAHMAN, R. icare: Applying iot technology for monitoring alzheimer’s patients. En *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, páginas 1–6. IEEE, 2018.
- ANTONIOLI, D. y TIPPENHAUER, N. O. Minicps: A toolkit for security research on cps networks. En *Proceedings of the First ACM workshop on cyber-physical systems-security and/or privacy*, páginas 91–100. 2015.
- ANWAR, Z. y MALIK, A. W. Can a ddos attack meltdown my data center? a simulation study and defense strategies. *IEEE Communications Letters*, vol. 18(7), páginas 1175–1178, 2014.
- ARORA, K., KUMAR, K., SACHDEVA, M. ET AL. Impact analysis of recent ddos attacks. *International Journal on Computer Science and Engineering*, vol. 3(2), páginas 877–883, 2011.

- ARSHAD, R., ZAHOOR, S., SHAH, M. A., WAHID, A. y YU, H. Green iot: An investigation on energy saving practices for 2020 and beyond. *IEEE Access*, vol. 5, páginas 15667–15681, 2017.
- BANGOR, A., KORTUM, P. T. y MILLER, J. T. An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction*, vol. 24(6), páginas 574–594, 2008.
- BASSOLI, M., BIANCHI, V. y MUNARI, I. D. A plug and play iot wi-fi smart home system for human monitoring. *Electronics*, vol. 7(9), página 200, 2018.
- BAYS, H. E., CHAPMAN, R., GRANDY, S. y GROUP, S. I. The relationship of body mass index to diabetes mellitus, hypertension and dyslipidaemia: comparison of data from two national surveys. *International journal of clinical practice*, vol. 61(5), páginas 737–747, 2007.
- BECKER, E., METSIS, V., ARORA, R., VINJUMUR, J., XU, Y. y MAKEDON, F. Smartdrawer: Rfid-based smart medicine drawer for assistive environments. En *Proceedings of the 2nd international Conference on Pervasive Technologies Related to Assistive environments*, páginas 1–8. 2009.
- BILLIARD, M. *Sleep: physiology, investigations, and medicine*. Springer, 2003.
- BLEDA, A. L., FERNÁNDEZ-LUQUE, F. J., ROSA, A., ZAPATA, J. y MAESTRE, R. Smart sensory furniture based on wsn for ambient assisted living. *IEEE Sensors Journal*, vol. 17(17), páginas 5626–5636, 2017.
- CALDERON, C., FORNS, M. y VAREA, V. Implication of the anxiety and depression in eating disorders of young obese. *Nutricion hospitalaria*, vol. 25(4), páginas 641–647, 2010.
- CARDIN, O. Classification of cyber-physical production systems applications: Proposition of an analysis framework. *Computers in Industry*, vol. 104, páginas 11–21, 2019.
- CECIL, J., ALBUHAMOOD, S., RAMANATHAN, P. y GUPTA, A. An internet-of-things (iot) based cyber manufacturing framework for the assembly of microdevices. *International Journal of Computer Integrated Manufacturing*, vol. 32(4-5), páginas 430–440, 2019.
- CHEN, B., YANG, Z., HUANG, S., DU, X., CUI, Z., BHIMANI, J., XIE, X. y MI, N. Cyber-physical system enabled nearby traffic flow modelling for autonomous vehicles. En *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, páginas 1–6. IEEE, 2017.

- CHEN, M., MA, Y., SONG, J., LAI, C.-F. y HU, B. Smart clothing: Connecting human with clouds and big data for sustainable health monitoring. *Mobile Networks and Applications*, vol. 21(5), páginas 825–845, 2016.
- CHO, S. y DHINGRA, V. Street lighting control based on lonworks power line communication. En *2008 IEEE International Symposium on Power Line Communications and Its Applications*, páginas 396–398. IEEE, 2008.
- COOPER, P. J. y TAYLOR, M. J. Body image disturbance in bulimia nervosa. *The British Journal of Psychiatry*, vol. 153(S2), páginas 32–36, 1988.
- COURTNEY, E. A., GAMBOZ, J. y JOHNSON, J. G. Problematic eating behaviors in adolescents with low self-esteem and elevated depressive symptoms. *Eating behaviors*, vol. 9(4), páginas 408–414, 2008.
- CULJAK, I., ABRAM, D., PRIBANIC, T., DZAPO, H. y CIFREK, M. A brief introduction to opencv. En *2012 proceedings of the 35th international convention MIPRO*, páginas 1725–1730. IEEE, 2012.
- DIXON, S. A., MENKEDICK, D. J., JACQUES, W. L., JONES, J. W., FINDLAY, J. K., WILKER JR, J., OSBORNE, E. E. y RILEY, C. W. Patient position detection apparatus for a bed. 2001. US Patent 6,208,250.
- DOLIC, Z., CASTRO, R. y MOARCAS, A. Robots in healthcare: a solution or a problem? *Policy Department for Economic, Scientific and Quality of Life Policies, Directorate General for Internal Policies, European Parliament*, 2019.
- EL-NAHAS, M., EL-SHAZLY, S., EL-GAMEL, F., MOTAWEA, M., KYRILLOS, F. y IDREES, H. Relationship between skin temperature monitoring with smart socks and plantar pressure distribution: A pilot study. *Journal of wound care*, vol. 27(8), páginas 536–541, 2018.
- ETELÄPERÄ, M., VECCHIO, M. y GIAFFREDA, R. Improving energy efficiency in iot with re-configurable virtual objects. En *2014 IEEE World Forum on Internet of Things (WF-IoT)*, páginas 520–525. IEEE, 2014.
- FAGAN, A. M., MINTUN, M. A., MACH, R. H., LEE, S.-Y., DENCE, C. S., SHAH, A. R., LAROSSA, G. N., SPINNER, M. L., KLUNK, W. E., MATHIS, C. A. ET AL. Inverse relation between in vivo amyloid imaging load and cerebrospinal fluid a β 42 in humans. *Annals of neurology*, vol. 59(3), páginas 512–519, 2006.
- FARZI, A., HASSAN, A. M., ZENZ, G. y HOLZER, P. Diabetes and mood disorders: Multiple links through the microbiota-gut-brain axis. *Molecular aspects of medicine*, vol. 66, páginas 80–93, 2019.

- FERDOUSH, S. y LI, X. Wireless sensor network system design using raspberry pi and arduino for environmental monitoring applications. *Procedia Computer Science*, vol. 34, páginas 103–110, 2014.
- FLEGAL, K. M., GRAUBARD, B. I., WILLIAMSON, D. F. y GAIL, M. H. Excess deaths associated with underweight, overweight, and obesity. *Jama*, vol. 293(15), páginas 1861–1867, 2005.
- GANESH, G., JAIDURGAMOHAN, K., SRINU, V., KANCHARLA, C. R. y SURESH, S. V. Design of a low cost smart chair for telemedicine and iot based health monitoring: An open source technology to facilitate better healthcare. En *2016 11th International Conference on Industrial and Information Systems (ICIIS)*, páginas 89–94. IEEE, 2016.
- GARCÍA-CRUZ, E., BRETONNET, A. y ALCARAZ, A. Testing smart glasses in urology: clinical and surgical potential applications. *Actas Urológicas Españolas (English Edition)*, vol. 42(3), páginas 207–211, 2018.
- GARCÍA-MAGARIÑO, I., LACUESTA, R. y LLORET, J. Agent-based simulation of smart beds with internet-of-things for exploring big data analytics. *IEEE Access*, vol. 6, páginas 366–379, 2017.
- GOOSSENS, L., BRAET, C., VAN VLIERBERGHE, L. y MELS, S. Weight parameters and pathological eating as predictors of obesity treatment outcome in children and adolescents. *Eating behaviors*, vol. 10(1), páginas 71–73, 2009.
- GREEN, R. C., WANG, L. y ALAM, M. Applications and trends of high performance computing for electric power systems: Focusing on smart grid. *IEEE Transactions on Smart Grid*, vol. 4(2), páginas 922–931, 2013.
- GUBBI, J., BUYYA, R., MARUSIC, S. y PALANISWAMI, M. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, vol. 29(7), páginas 1645–1660, 2013.
- HAQUE, S. A. y AZIZ, S. M. False alarm detection in cyber-physical systems for healthcare applications. *Aasri Procedia*, vol. 5, páginas 54–61, 2013.
- HASSANNEJAD, H., MATRELLA, G., CIAMPOLINI, P., MUNARI, I. D., MORDONINI, M. y CAGNONI, S. A new approach to image-based estimation of food volume. *Algorithms*, vol. 10(2), página 66, 2017.
- HATZIVASILIS, G., PAPAEFSTATHIOU, I. y MANIFAVAS, C. Real-time management of railway cps secure administration of iot and cps infrastructure. En *2017 6th Mediterranean conference on embedded computing (MECO)*, páginas 1–4. IEEE, 2017.

- HE, Z., WANG, M., XIE, Q., WANG, G., ZHAO, Y., LIAN, Y., MENG, B. y PENG, Z. A heart rate measurement system based on ballistocardiogram for smart furniture. En *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, páginas 151–154. IEEE, 2018.
- ISHII, H., KIMINO, K., ALJEHANI, M., OHE, N. y INOUE, M. An early detection system for dementia using the m2 m/iot platform. *Procedia Computer Science*, vol. 96, páginas 1332–1340, 2016.
- IZQUIERDO, L. R., GALÁN, J. M., SANTOS, J. I. y DEL OLMO, R. Modelado de sistemas complejos mediante simulación basada en agentes y mediante dinámica de sistemas. *EMPIRIA. Revista de Metodología de las Ciencias Sociales*, (16), páginas 85–112, 2008.
- JASSAS, M. S., QASEM, A. A. y MAHMOUD, Q. H. A smart system connecting e-health sensors and the cloud. En *2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE)*, páginas 712–716. IEEE, 2015.
- JIA, X., FENG, Q., FAN, T. y LEI, Q. Rfid technology and its applications in internet of things (iot). En *2012 2nd international conference on consumer electronics, communications and networks (CECNet)*, páginas 1282–1285. IEEE, 2012.
- JOHNSON, K. A. Amyloid imaging of alzheimer’s disease using pittsburgh compound b. *Current neurology and neuroscience reports*, vol. 6(6), páginas 496–503, 2006.
- KASINATHAN, P., PASTRONE, C., SPIRITO, M. A. y VINKOVITS, M. Denial-of-service detection in 6lowpan based internet of things. En *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*, páginas 600–607. IEEE, 2013.
- KAUR, N. y SOOD, S. K. An energy-efficient architecture for the internet of things (iot). *IEEE Systems Journal*, vol. 11(2), páginas 796–805, 2015.
- KHATTAK, H. A., SHAH, M. A., KHAN, S., ALI, I. y IMRAN, M. Perception layer security in internet of things. *Future Generation Computer Systems*, vol. 100, páginas 144–164, 2019.
- KUMAR, S., SAHOO, S., MAHAPATRA, A., SWAIN, A. K. y MAHAPATRA, K. K. Security enhancements to system on chip devices for iot perception layer. En *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, páginas 151–156. IEEE, 2017.
- LABEODAN, T., ADUDA, K., ZEILER, W. y HOVING, F. Experimental evaluation of the performance of chair sensors in an office space for occupancy

- detection and occupancy-driven control. *Energy and Buildings*, vol. 111, páginas 195–206, 2016.
- LAHIRI, D. K. y MALONEY, B. Beyond the signaling effect role of amyloid- β 42 on the processing of app, and its clinical implications. *Experimental neurology*, vol. 225(1), páginas 51–54, 2010.
- LEE, J., BAGHERI, B. y KAO, H.-A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, vol. 3, páginas 18–23, 2015.
- LEE, Y.-D. y CHUNG, W.-Y. Wireless sensor network based wearable smart shirt for ubiquitous health and activity monitoring. *Sensors and Actuators B: Chemical*, vol. 140(2), páginas 390–395, 2009.
- LI, F., SHINDE, A., SHI, Y., YE, J., LI, X.-Y. y SONG, W. System statistics learning-based iot security: Feasibility and suitability. *IEEE Internet of Things Journal*, vol. 6(4), páginas 6396–6403, 2019.
- LOUNIS, A., HADJIDJ, A., BOUABDALLAH, A. y CHALLAL, Y. Secure and scalable cloud-based architecture for e-health wireless sensor networks. En *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, páginas 1–7. IEEE, 2012.
- LUND, A. M. Measuring usability with the use questionnaire12. *Usability interface*, vol. 8(2), páginas 3–6, 2001.
- MADDIKUNTA, P. K. R., SRIVASTAVA, G., GADEKALLU, T. R., DEEPA, N. y BOOPATHY, P. Predictive model for battery life in iot networks. *IET Intelligent Transport Systems*, vol. 14(11), páginas 1388–1395, 2020.
- MAJEED, Q., HBAIL, H. y CHALECHALE, A. A comprehensive mobile e-healthcare system. En *2015 7th Conference on Information and Knowledge Technology (IKT)*, páginas 1–4. IEEE, 2015.
- MAN, K. L., TING, T., KRILAVIČIUS, T., WAN, K., CHEN, C., CHANG, J. y POON, S.-H. Towards a hybrid approach to soc estimation for a smart battery management system (bms) and battery supported cyber-physical systems (cps). En *2012 2nd Baltic Congress on Future Internet Communications*, páginas 113–116. IEEE, 2012.
- MERLO, C., ABI AKLE, A., LLARIA, A., TERRASSON, G., VILLENEUVE, E. y PILNIERE, V. Proposal of a user-centred approach for cps design: pillbox case study. *IFAC-PapersOnLine*, vol. 51(34), páginas 196–201, 2019.
- MINTUN, M., LAROSSA, G., SHELINE, Y., DENCE, C., LEE, S. Y., MACH, R., KLUNK, W., MATHIS, C., DEKOSKY, S. y MORRIS, J. [11c] pib in a nondemented population: potential antecedent marker of alzheimer disease. *Neurology*, vol. 67(3), páginas 446–452, 2006.

- MIRKOVIC, J. y REIHER, P. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, vol. 34(2), páginas 39–53, 2004.
- MORENO, M., ÚBEDA, B., SKARMETA, A. F. y ZAMORA, M. A. How can we tackle energy efficiency in iot based smart buildings? *Sensors*, vol. 14(6), páginas 9582–9614, 2014.
- MORÓN, C., PAYÁN, A., GARCÍA, A. y BOSQUET, F. Domotics project housing block. *Sensors*, vol. 16(5), página 741, 2016.
- NAM, H., KIM, J.-H. y KIM, J.-I. Smart belt: A wearable device for managing abdominal obesity. En *2016 International Conference on Big Data and Smart Computing (BigComp)*, páginas 430–434. IEEE, 2016.
- ODDY, W. H., ROBINSON, M., AMBROSINI, G. L., THERESE, A., DE KLERK, N. H., BEILIN, L. J., SILBURN, S. R., ZUBRICK, S. R., STANLEY, F. J. ET AL. The association between dietary patterns and mental health in early adolescence. *Preventive medicine*, vol. 49(1), páginas 39–44, 2009.
- PARK, B. K., JEON, B. y KIM, R. Improvement practices in the performance of a cps multiple-joint robotics simulator. *Applied Sciences*, vol. 10(1), página 185, 2020.
- PERAITA-ADRADOS, R. Avances en el estudio de los trastornos del sueño. *Rev Neurol*, vol. 40(8), páginas 485–91, 2005.
- PRENTICE, A. M. y JEBB, S. A. Beyond body mass index. *Obesity reviews*, vol. 2(3), páginas 141–147, 2001.
- QIU, H., QIU, M., LIU, M. y MEMMI, G. Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. *IEEE journal of biomedical and health informatics*, vol. 24(9), páginas 2499–2505, 2020.
- RAD, C.-R., HANCU, O., TAKACS, I.-A. y OLTEANU, G. Smart monitoring of potato crop: a cyber-physical system architecture model in the field of precision agriculture. *Agriculture and Agricultural Science Procedia*, vol. 6, páginas 73–79, 2015.
- RAMÍREZ, P. L. G., TAHA, M., LLORET, J. y TOMÁS, J. An intelligent algorithm for resource sharing and self-management of wireless-iot-gateway. *IEEE Access*, vol. 8, páginas 3159–3170, 2019.
- RECHTSCHAFFEN, A. A manual for standardized terminology, techniques and scoring system for sleep stages in human subjects. *Brain information service*, 1968.

- RENTZ, D. M., AMARIGLIO, R. E., BECKER, J. A., FREY, M., OLSON, L. E., FRISHE, K., CARMASIN, J., MAYE, J. E., JOHNSON, K. A. y SPERLING, R. A. Face-name associative memory performance is related to amyloid burden in normal elderly. *Neuropsychologia*, vol. 49(9), páginas 2776–2783, 2011.
- SAIFUZZAMAN, M., MOON, N. N. y NUR, F. N. Iot based street lighting and traffic management system. En *2017 IEEE region 10 humanitarian technology conference (R10-HTC)*, páginas 121–124. IEEE, 2017.
- SÁNCHEZ BENITO, J. y PONTES TORRADO, Y. Influencia de las emociones en la ingesta y control de peso. *Nutrición hospitalaria*, vol. 27(6), páginas 2148–2150, 2012.
- SANDROFF, B. M., WYLIE, G. R., SUTTON, B. P., JOHNSON, C. L., DELUCA, J. y MOTL, R. W. Treadmill walking exercise training and brain function in multiple sclerosis: preliminary evidence setting the stage for a network-based approach to rehabilitation. *Multiple Sclerosis Journal—Experimental, Translational and Clinical*, vol. 4(1), página 2055217318760641, 2018.
- SASSO, A. T. L. y BUCHMUELLER, T. C. The effect of the state children’s health insurance program on health insurance coverage. *Journal of health economics*, vol. 23(5), páginas 1059–1082, 2004.
- SETHI, P. y SARANGI, S. R. Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, vol. 2017, 2017.
- SOGI, N. R., CHATTERJEE, P., NETHRA, U. y SUMA, V. Smarisa: a raspberry pi based smart ring for women safety using iot. En *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, páginas 451–454. IEEE, 2018.
- SPILLMANJR, W., MAYER, M., BENNETT, J., GONG, J., MEISSNER, K., DAVIS, B., CLAUS, R., MUELENAERJR, A. y XU, X. A ‘smart’bed for non-intrusive monitoring of patient physiological factors. *Measurement Science and Technology*, vol. 15(8), página 1614, 2004.
- STANEK, J. y KENCL, L. Sipp-dd: Sip ddos flood-attack simulation tool. En *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, páginas 1–7. IEEE, 2011.
- STEURER, P. y SRIVASTAVA, M. B. System design of smart table. En *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.(PerCom 2003)*., páginas 473–480. IEEE, 2003.

- THONGKHAO, Y. y PORA, W. A low-cost wi-fi smart plug with on-off and energy metering functions. En *2016 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, páginas 1–5. IEEE, 2016.
- TORRES-SANZ, V., SANGUESA, J. A., MARTINEZ, F. J., GARRIDO, P. y MARQUEZ-BARJA, J. M. Enhancing the charging process of electric vehicles at residential homes. *IEEE Access*, vol. 6, páginas 22875–22888, 2018.
- VAN KRANENBURG, R. y BASSI, A. Iot challenges. *Communications in Mobile Computing*, vol. 1(1), páginas 1–5, 2012.
- VARATHARAJAN, R., MANOGARAN, G., PRIYAN, M. K. y SUNDARASEKAR, R. Wearable sensor devices for early detection of alzheimer disease using dynamic time warping algorithm. *Cluster Computing*, vol. 21(1), páginas 681–690, 2018.
- WANG, J., ABID, H., LEE, S., SHU, L. y XIA, F. A secured health care application architecture for cyber-physical systems. *arXiv preprint arXiv:1201.0213*, 2011.
- WHITEHOUSE, S., YORDANOVA, K., LUDTKE, S., PAIEMENT, A. y MIRMEHDI, M. Evaluation of cupboard door sensors for improving activity recognition in the kitchen. En *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, páginas 167–172. IEEE, 2018.
- WU, F.-J., KAO, Y.-F. y TSENG, Y.-C. From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile computing*, vol. 7(4), páginas 397–413, 2011.
- YOUSEFI, R., OSTADABBAS, S., FAEZIPOUR, M., NOURANI, M., NG, V., TAMIL, L., BOWLING, A., BEHAN, D. y POMPEO, M. A smart bed platform for monitoring & ulcer prevention. En *2011 4th international conference on biomedical engineering and informatics (BMEI)*, vol. 3, páginas 1362–1366. IEEE, 2011.
- ZHANG, Y., QIU, M., TSAI, C.-W., HASSAN, M. M. y ALAMRI, A. Health-cps: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal*, vol. 11(1), páginas 88–95, 2015.
- ZHANG, Y., ZHU, Z. y LV, J. Cps-based smart control model for shop-floor material handling. *IEEE Transactions on Industrial Informatics*, vol. 14(4), páginas 1764–1775, 2017.

ZHOU, B., CHENG, J., SUNDHOLM, M., REISS, A., HUANG, W., AMFT, O. y LUKOWICZ, P. Smart table surface: A novel approach to pervasive dining monitoring. En *2015 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, páginas 155–162. IEEE, 2015.